Supreme Court, U.S.
FILED
06122 2007 30 2008
OFFICE OF THE CLERK

No._____

In the Supreme Court of the United States

EBBIE PAUL MUNOZ, PRO SE, *Petitioner*

v.

CENTRAL TELEPHONE COMPANY NEVADA; ET AL
-Respondents

On Petition for a Writ of Certiorari to the United States Court of Appeals for the 9th Circuit

PETITION FOR WRIT OF CERTIORARI

EBBIE PAUL MUNOZ ; Pro Se
P.O. BOX 61311
LAS VEGAS, NEVADA 89160
702-207-6111

QUESTIONS PRESENTED

Does the P.U.C. have the right to deny consumers' rights to a fair and equal right of protection under the CONSTITUTION'S AMENDMENTS 5 and 14, without proper due process of law? Do they have the right to close doors on intrastate and interstate issues of the most difficult cases of the system? Are they powerful enough to allow Telco's to act in a criminal manner? Can the P.U.C. legally overlook procedures in reference to records, witnessing, arbitrary and capricious acts? Does the P.U.C., an administrative state agency, have the force of law to stone wall consumers and rule over Federal Jurisdiction in toll-fraud cases? Does Sprint have the right to deny law enforcement officers records? Does the P.U.C. have to put burden of evidence on Mobroz? Can the P.U.C. be reviewed under arbitrary and capricious acts? Did Sprint have the right to deny their responsibility and jeopardize national security?

PARTIES

The Petitioner, he is the licensed owner of Las Vegas, Informer, an adult entertainment business in Las Vegas, Nevada, 1516 E Tropicana #151, 89119. Upon information and belief of the petitioner the respondent, SPRINT TELEPHONE CO. is a licensed carrier in the State of Nevada (Las Vegas). Sprint is the company responsible for the lack of security and daily operations of the phone lines sold, to the petitioner at times, specified herein and as up to today are owners of all cable and faculties of unsecured network (See Appendix L).

TABLE OF CONTENTS

QUESTIONS PRESENTED.....i
PARTIES.....ii
TABLE OF CONTENTS.....iii
ISSUES ADDRESSED.....iii
INDEX TO APPENDIXES.....iv
TABLE OF AUTHORITIES.....ix
STATUES AND RULES.....x
OPINIONS BELOW.....1
JURISDICTION.....2
CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED.....2
STATEMENT OF THE CASE.....7
REASONS FOR GRANTING THE WRIT.....9
CONCLUSION.....11
DECLARATION IN SUPPORT.....13
PROOF OF SERVICE.....14

ISSUES ADDRESSED

ISSUES **PAGE NUMBER**

1. ENDANGERMENT TO NATIONAL SECURITY.....1-12

2. ARBITRARY AND CAPRICIOUS ACTS.....1
   a. REVIEW OF ABUSE AND INDISCRETION OF THE P.U.C.....1 & 12

3. RIGHT TO FAIR HEARING.....1-2
   a. RIGHT TO HAVE EVIDENCE, BOOKS, AND RECORDS PRODUCED.....1-2, 4-5, 8,10-12
   b. RIGHT TO SUBPOENA WITNESSES.....1, 6, 8

4. UNFAIR TRADE PRACTICES.....1, 9-12

a. LACK OF CONSUMERS PROTECTION.....1-12
b. INTERFERENCE OF COMMERCE.....1-2, 6, 11-12

5. STATUTES OF LIMITATION.....1 & 3
a. INTERSTATE AND INTRASTATE.....1, 4-5 & 9
b. TOLL FRAUD AND SLAMMING.....1, 6-7

INDEX TO APPENDIXES

APPENDIX A REGULATORY OPERATION STAFF'S POST-HEARING BRIEF.....1a-16a

APPENDIX B REGULATORY OPERATIONS STAFF'S MOTION TO DESIGNATE CONFIDENTIAL INFORMATION AND MOTION TO ISSUE PROTECTIVE ORDER.....17a-19a

APPENDIX C INTERIM ORDER DENYING MOTION FOR PROTECTIVE ORDER AND DENYING MOTION TO COMPEL.....20a-23a

APPENDIX D PUBLIC UTILITIES COMMISSION ORDER 24a-28a

APPENDIX E ORDER GRANTING DEFENDANT'S MOTION TO DISMISS WITH PREJUDICE.....29a-35a

APPENDIX F UNITED STATES COURT OF

APPEALS FOR THE NINTH CIRCUIT ORDER.....36a

APPENDIX G APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEVADA 37a-38a

APPENDIX H UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT: JUDGMENT.....39a

APPENDIX I UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT ORDER.....40a

JOINT APPENDIX
VOLUME 1
APPENDIXES J-K-L-M
PGS A-42-111

APPENDIX J PGS-42-68
MEMORANDUM OF LAW IN SUPPORT OF INFORMAL BRIEF

APPENDIX K PGS A-69-83
P.U.C. DOCKET 00-6057
BATES RECORD 010512-010533
KANSAS CITY NETWORK
INTRASTATE –INTERSTATE
DOCUMENTED SS7 INTRUSION
EVENT P.U.C. DEPOSITIONS
BATES RECORD 011400-011401-
011408.....

APPENDIX L PGS A- 84-97
SPRINT NETWORK
P.U.C. DOCKET 00-60

SPRINT MONOPOLY ARTICLE
REVIEW JOURNAL NEWSPAPER
.....PGS A-97-101

APPENDIX M PGS-102-111
P.U.C. DOCKET 00-6057
NATIONAL SECURITY
BATES RECORD 010008
.....PGS A-103-104
TERRORIST ISSUES
TRANSCRIPTS OF HEARING 10;
02 AM. MARCH 14, 2002
.....PGS A-105-111

JOINT APPENDIX
VOLUME 2
APPENDIXES N-O
PGS-A -112-162

APPENDIX N PGS A-112-133
P.U.C. DOCKET 00-6057
EXPERT WITNESSES BATES
RECORD 005656-008660
KEVIN MITNICK DIRECT
TESTIMONY.....PGS -A-112-117
P.U.C. DIRECT TESTIMONY
RON BARDARSON
EXPERT WITNESS
P.U.C. STAFF.....PGS A – 118 - 133

APPENDIX O PGS A 134- 162
P.U.C. DOCKET 00-6057
CLOSING ARGUMENTS OF
EDDIE MUNOZ AUG-16-2002
.....PGS A-135-146
P.U.C. DOCKET REBUTTAL
TESTIMONY OF SCOTT COLLINS
REBUTTAL TESTIMONY FROM

EDDIE MUNOZ.....PGS A-147 - 162

JOINT APPENDIX
VOLUME 3
APPENDIXES P
PGS –A-163 -217

APPENDIX P PGS A – 163-217
NATIONAL SECURITY
FEDERAL ENVIRONMENT
.....PGS A-164-168
FEDERAL ARREST
F.B.I. STRIKE FORCE
.....PGS A – 169-195
FEDERAL INVESTIGATION
P.U.C. DOCKET 00-6057
DIVERSION BATES RECORD
01365-101368.....PGS A - 196-217

JOINT APPENDIX
VOLUME 4
APPENDIXES Q-R-S-T
PGS A-218--341

APPENDIX Q PGS A -218-226
UNITED STATES DISTRICT
COURT HEARING TRANSCRIPT
OF 1-24-2005 9: 35 AM

APPENDIX R PGS A-227-242
SPRINT TROUBLE TICKETS
SHOW PROBABLE CAUSE
PROBLEM EXISTS UP TO DATE

APPENDIX S PGS A-243-253
EMBARQ TROUBLE TICKETS
SHOW PROBABLE CAUSE
SHELL GAME PROBLEM EXIST
UP TO DATE

APPENDIX T PGS A-254-269
NATIONAL SECURITY ISSUES
CYBER WAR SECURING SS7
TELECOMMUNICATIONS
NETWORKS

JOINT APPENDIX
VOLUME 5
APPENDIXES U-V-W-X
PGS-A-270 - 339

APPENDIX U PGS A-270-282
P.U.C. DOCKET.00-6057
BATES RECORD 010420 – 10438
FCC. SLAMMING INCIDENTS
TOLL FRAUD EXHIBIT
DOCUMENTED EVENT
INTERSTATE 800 NUMBERS
PREEMPTS FEDERAL
JURISDICTION

APPENDIX V PGS A- 283-288
SECRET SERVICE
CORRESPONDENCE....PGS A-284-285
F.C.C. CORRESPONDENCE
.....PGS A-286-287
SECURITIES EXCHANGE
COMMISSION WASHINGTON D.C.
.....PGS-A-288

APPENDIX W PGS –A-289-293
UNITED STATES SENATOR
HARRY REID U.S. SENATOR
PUBLIC HEARING
APRIL 13 2006 5:30 PM
PUBLIC STATEMENT
SENATOR REQUEST

APPENDIX X PGS-A-294-339
STATE OF NEVADA OFFICE
OF THE ATTORNEY GENERAL
CYBER CRIME NEVADA TASK
FORCE.....PGS –A-295-327
P.U.C. DOCKET 00-6057
BATES RECORD 010022-010028
DANIEL A MORRIS
ASSISTANT UNITED STATES
ATTORNEY COMPUTER AND
TELECOMMUNICATIONS
COORDINATOR.....PGS A-328-339

TABLE OF AUTHORITIES CITED

CASES **PAGE NUMBER**

SOUTHWESTERN BELL vs. PUBLIC UTILITIES COMMISSION 208, F2d475 (5th 2000).....2

PACIFIC BELL vs. PAC WEST TELECOMM.INC.325 F.2d 1114 (9th cir 2000).....2

US WEST vs. SPRINT COMMUNICATION 75 F3d.124 (10th2002.....2

BOUNDS vs. SMITH U.S. SUPREME COURT RULING 4

DE LOREAN MOTOR CO 991.F2D1236 (6TH CIR 1993 AT.1240.....5

LAWDER vs. MARSHALL 898 F2D 11961199 (6TH CIR 1990.....5

BERON WEINER GLICK AND BROOK vs.

MANUFACTURES HANOVER TRUST COND ILL 1993, 818 F SUPP 1152.....5

CAPPADORA vs. CELE BREZZE 356 F2D1(2ND CIR 1966.....3

STUCKEY vs. WINBERGER 488 FEDERAL REPORTER 2 D series 909.3.....3

STORER BROADCASTING CO. vs. US DIST/COL 1956 76 SCI 763 351 US 192 100 LED 1081.....4

US vs. CLAYTON ACT 108 F3D 1114 1117 9TH CIR SEC 12-27 TITLE 15.....4

VAN DUSSEN -STORA MOTOR INN vs. ROCHESTER TELEPHONE CORP 1972.338.NYS.2d31.72.....4

FEDERAL COMMUNICATION ACT FCA MFS INTERN.INC VINTEWATIONAL TELCOM LTD, ED VA 1999, SO F SUPP.2D 517.....3

ADMISTRATIVE PROCEDURE ACT CAPA 5 USC 701 -706 APA AUTHORIZES JUDICIAL REVIEWS..... 3

STATUES AND RULES

TITLE 42 USCA HEALTH , WELFARE AND SAFETY 2

TITLE 47 USCA 1004.....8
TITLE 47 USCA SEC 202.....1
TITLE 47 USCA SEC 1331.....1
TITLE 47 USCA SEC 1338.....1
TITLE 47 USCA SEC 251, 252, 263 2
TITLE 47 USCA SEC 229 B.....8

NRS 703.340 703.195 703.190 703.196 703.373 SEC 6 A-F 703.370 703.340.703.350.....4-5

OTHER

Whistle Blower Act (Policy 2.06 Sec 554.001 Government Code).....2

STATE OF NEVADA DISTRICT COURT CASE NO. A 401763.....8

STATE OF NEVADA DISTRICT COURT CASE NO. A 419237.....8

OPINIONS BELOW

Regulatory Operations Staff's motion to designate confidential information and motion to issue protective order – October 31, 2001

Interim order denying motion for protective order and denying motion to compel was entered on April 1, 2002

The Public Utilities Commission- Regulatory Operations Staff's Post-Hearing Brief - August 16, 2002

The Public Utilities Commission- order was entered on September 23, 2002.

The Public Utilities Commission- appeal was invoked at September 23, 2002.

The Public Utilities Commission- motion for appeal was denied the same day, September 23, 2002.

United States District Court of Southern Nevada- complaint for recovery of damages was filed on August 30, 2004.

United States District Court - Oral argument was held on January 24, 2005

United States District Court - Dismissal of Complaint was filed on February 8, 2005.

Appeal to the United States 9th Circuit Court of Appeals was filed on September 28, 2005.

United States 9th Circuit Court- Judgment was entered March 29, 2006.

A petition for rehearing en banc was filed on April 17, 2006.

Denial for the petition for rehearing en banc was filed on July 31, 2006

JURISDICTION AND VENUE

Pursuant to 28 U.S.C.A. 1746, Petitioner brings forth this petition for a writ of Certiorari in a timely action for **RECOVERY OF DAMAGES** pursuant to the laws of the United States **47 U.S.C.A. Sec.207.** This Court has subject matter jurisdiction under **28 U.S.C.A. Sec.1331 and 28 U.S.C.A. Sec.1338.** This Court has personal Jurisdiction over the Respondent Sprint Telephone Company where they are licensed in the State of Nevada (Las Vegas) as a Carrier under both under state and federal jurisdiction of interstate and intrastate.

CONSTITUTION AND STATUTORY PROVISIONS INVOLVED

Munoz does not believe that congress would have wished to close the doors of the courts to the petitioner. His claim for relief under his constitutional rights under the U.S. codes was NEVER rebutted and Sprint NEVER handed over vital information to the P.U.C. STAFF. They destroyed records in the case, used oppression of their office to keep employees quiet or lose their jobs. Sprint threatened P.U.C. staff, stating they would sue the P.U.C. for being mistreated. In an ex parte meeting with Commission members behind closed doors, Sprint would use their political POWER. They could lose their jobs; **The Whistle Blower Act (Policy 2.06 Sec 554.001 Government code)** should step up for the abuse to the public (See Appendix J-A-43-60, O-A-134-162). An administrative hearing, which was denied over deceit and failure to produce vital records, proved Munoz' case to have arbitrary and,

capricious standards of review. See **Southwestern Bell v. Public Utilities Commission 208 F.2d 475(5TH 2OOO) THE COURT IN PACIFIC BELL V. PAC WEST TELECOMM. INC. 325 F.2d 1114 (9th cir 2000). US West vs. Sprint (cite 275 F.3d1241.)(10th Circuit 2002):** which addressed the force of law of the P.U.C. rulings; thus making the final order of P.U.C. stand without the force of law. The decision, absent to the contrary, Congress may rather be presumed to have intended courts should fulfill their traditional role of defining and maintaining the proper bounds of administrative discretion and safeguarding the rights of the individual, of consumers fraud against unfair trade acts, causing INTERFERENCE OF COMMERCE towards the public (See Appendix P- A-163-217).

The telecommunication act, **title 47 U.S.C.251, 252,263A,** with the guidance of the FCC, is to PROTECT the PUBLIC. Not to destroy or to endanger national security (see Appendix T-A-254-269). CONGRESS DID NOT INTEND TO BAR JUDICIAL REVIEW OF THE P.U.C. IN CERTAIN CASES. The AGGRIEVED petitioner made all Filing dates for state and federal statues of limitation of 2 years for recovery of damages under **USCA TITLE 47 ACT SEC 207. UNDER DIRECTION OF LEGAL CONSUL. STUCKEY vs. WINBERGER 488 FEDERAL REPORTER 2D SERIES 909, 3 Cite; Cappadora v. Celebrezze, 356 F.2d 1(2D CIR. 1966)** He argues that decisions not to reopen are reviewable, for abuses of discretion, under the **administrative procedure ACT. ("APA") (5 USC. 701-706.**

The APA authorizes judicial review of "final agency action for which there is no adequate remedy in a court. This last attempt for someone to do their job and understand the importance of the basis of this cry for help is not just for the petitioner, but also for the public safety of networks. Networks that hold important databases accessed by telecommunication switches that hold us from terrorist groups of cyber war that have access to SS7 network WHICH IS THE BACKBONE OF THE

TELECOMMUNICATION OF THE US. (See Appendix T-A-254-269). P.U.C. FACTS and FINDINGS of Staff (See Appendix A 1a-16a) show the need of the review of the procedures and standards to insure the public integrity in the P.U.C. They are brushing this issue under the carpet, complaints keep generating in Nevada, and to understand that nobody can get any relief until Sprint realizes they are not above the law and they should take responsibility for the unsecured network and help protect customers from inland terrorist groups of the world today. TO GET SPRINT TO HELP IN THIS MATTER TODAY IS MORE DIFFICULT, DUE TO SPRINT PLAYING a SHELL GAME TO THE PUBLIC. SPRINT HAS SHUT DOWN THEIR SECURITY OFFICE in NEVADA. In addition, Sprint WILL NOT work with any LAW officials (See Appendix M-A-102-111, N-A-112-A-133) and NOBODY knows what to do except for to HIDE THE ISSUE. It seems as if there is no protection for consumers.

Not even for the Secret Service Cyber Task Force (See Appendix V-A-283-288). This is an outcry for the public to review standards to mandate Telco's and their obligation of breach of contracts, security, background checks of switch engineers, and turn over records under seal if necessary. They failed to disclose information to all investigators and should have been sanctioned and fined for their actions (See Appendix N-112-133). In the P.U.C. hearing hiding its faults in a full administrative hearing making up rules as they go along and then do not enforce the ones on the books **NRS 703.370, NRS 703.340 NRS 703.195 NRS 703.190, NRS 703.196 703.350 703.340703 .196** Enforcement statues of the state of Nevada.

Today telephone issues, REACH NATION WIDE RAPIDLY ROBBING THE COUNTRY BLIND BY NETWORKS. The country NEEDS HELP to take back America from the criminals of today. Records on appeal fully state the impurities of Sprint and the P.U.C. As petitioner was aggrieved by commission and parties suffered legal wrong by action, under **title 47 sec 402, 122, 18** administrative provisions, A REVIEW IS

GRANTED **U.S. v STORER BROADCASTING CO.US.DIST COL.1956, 76 SCt. 763.351.U.S 192.100.LED 1081**. The National Telecommunications and Information Administration Organization Act enacted Title 47 under the Title 42 for the Public health, and welfare, Congress findings that Telecommunications and information are vital to the public and Welfare of National Security.

The competitiveness of the United States and the critical need for competent information polices are essential for branches of the Federal Government. The P.U.C.'s own facts and findings found Sprint security breaches of the ss7 network is the back bone of the infrastructure Jeopardized National Security (See Appendix M-A-102-111 A-A-16). The Interference of Commerce and Unfair Trade Laws should preempt federal jurisdiction UNDER THE CLAYTON ACT. **SEC 12-27 .of Title 15 Van Dussen -Stora Motor Inn v Rochester Tele phone Corp**. Petitioner was financially ruined by these proceedings and preceded in proper person to invoke his constitutional rights under United States Supreme Court rulings of **BOUNDS vs. SMITH**., to BRING these issue to light in a time of war (See Appendix Q-A-218-226).

To be barred by res judicata ruling. To bar petitioner from presenting his claims that were both intrastate and interstate issues, P.U.C. and Sprint's trickery knowing that issues were from state to state creating the wall to stay above the law the thousands of documents generated at P.U.C. hearing to document events. Preempt federal jurisdiction, to open the door to U.S. District Court. P.U.C. FEDERAL ISSUES were never resolved DUE TO PENDING FEDERAL FBI Strike Force AND HOMELAND SECURITY INVESTIGATIONS (See Appendix M-A-102-111-A-109, P-A-163-217).

In **RE DeLOREAN MOTOR CO.991 F.2d 1236, (6TH CIR.1993) AT 1240**; the court must construe the complaint in the light most favorable to the plaintiff, accept all factual allegations. As, and determine whether

the plaintiff undoubtedly can prove no set of facts in support of his CLAIMS THAT ENTITLE HIM TO RELIEF. Under **NRS 703.373 SEC 6** a, f, arbitrary or capricious ACTS characterized by abuse of discretion of confecting state and federal statues and procedures (See Appendix V-A-284-298, P-A-163-217). **LAWLER vs. MARSHALL, 898 F.2D 1196, 1199 (6th cir. 1990)** cite omitted; A complaint need only give "fair notice of what the plaintiff's claim is and the grounds upon which it rest." This petitioner has looked for the court to apply all the liberal standards that may apply when interpreting the claims before the court (**See Bercoon, Weiner, Glick and Brook v. Manufactures Hanover Trust Co,N.D.ILL 1993, 818 F ,SUPP.1152**) on a motion to dismiss for failure to state claim. The district court must interpret ambiguities in complaint in favor of plaintiff. Plaintiff is free in defending against motion to allege without evidentiary support any facts that they please that are consistent with complaint in order to show that there is state of facts, within the scope of the complaint in order to show that if proved would entitle them to judgment.

STATEMENT OF CASE

Munoz, Petitioner has operated several businesses in Clark County for, many years. In 1992, Munoz filed complaint with F.B.I. alleging that his incoming telephone calls routed through Sprints Network were being diverted to competitors. MUNOZ has filed complaints with F.C.C MUNOZ also FILED COMPLAINTS, SECRET SERVICE CYBER TASK FORCE. ORGANIZED CRIME STRIKE TASK FORCE, ATTORNEY GENERAL OFFICE, HOME LAND SECURITY, AND INLAND HOME LAND SECURITY, SECURITY EXCHANGE COMMISSION worked with officers on several investigations on an undercover basis putting, PETITIONER and family at risk after numerous subsequent contacts with officials. Sprint would not corporate with any law OFFICIAL or STAFF of the P.U.C. (See Appendix A-A-1-16 ,R-A-227-242, S-A-243-253) towards the security problem with no progress towards a solution. This problem has never been solved up to this date, with no adequate remedy at law, from the un-securing of business networks sold to consumers leaving no consumers protection. Lack of security to public networks, which also services State and Federal Government agencies are at risk and have been compromised (See Appendix L-A-85-101, P-A-163-217, **171**). The aggrieved petitioner was harmed by **ARBITRARY AND CAPRICIOUS ACTS OF THE P.U.C.** knowing the P.U.C. did not have the funds are the expertise to check network integrity. Without Sprint's corporation, it is impossible to solve the problem of the community since there were several complaints from different business such as: limos, cabs, pizza, bail bonds, private eyes, attorneys, and florists. These various businesses made consumer complaints with the P.U.C. **LAW OFFICIALS WERE DENIED TO TESTIFY AT THE LAST MINUTE DUE TO SPRINTS POLITICAL INFLUENCE.** These HOMELAND SECURITY officers had worked on cases that made

arrests of fired employees of Sprint the ongoing Federal Investigations (See Appendix P-A-163-217, J-A-42-68) involvement of cases of call diversion. This made the state P.U.C. hearing take a back seat, to the FBI Investigations (See Appendix P-A-163-217).

REASONS FOR GRANTING WRIT

Petitioner comes forth with said petition due to the times of War and the future nation's security rest on telecommunications of our daily lives. Phone lines and simple passwords access mainframe computers. After deregulation the technology has grown at a rapid rate, has ran off and left consumers behind has left the public at corporation mercy individuals don't have the expertise to check the integrity of Telco's or access, resources P.U.C. have to relie on the word of Sprint. Please(See Appendix J-A-42-68 and you will see that deceptive acts of Sprint, which crumbled the P.U.C.'s integrity towards the public UNDER TITLE, **47 SEC 229(b).**

Systems security and integrity, require Sprint to maintain secure and accurate records of any interception or access with or without such authorization of the Communications Assistance for law enforcement act [47 U.S.C.A. $ 1004] Sprint's lack of integrity needs to establish the appropriate polices and procedures for the supervision and control of its officers and employees.(See Appendix A-A-1-16 Conflicts of interest of parties of commission and the attorney general office due to the lawsuit filed by Petitioner commission should have hired an out side consul, as the petitioner worked on investigations with attorney general office. Commission used attorney general office as consul, which was a GREAT CONFLICT OF INTEREST. (See Appendix O-A-134-162) which lacked integrity to Petitioner? The P.U.C. has been stonewalling complaints since 1991 to the point of petitioner had to, file a writ of mandate on April 11,1999 (STATE OF NEVADA DISTRICT COURT CASE NO. A 401763) towards a solution , Petitioner voluntarily dismissed the case April 29,1999 When the commission agreed to investigate, After over one year of delay by the P.U.C. .Petitioner filed another writ of mandate on May 19, 2000(STATE OF NEVADA DISTRICT COURT CASE NO. A 419237) Petitioners rights kept being violated by oppression under color of office. Petitioner was seeking commission to hold

a public hearing to investigate the numerous complaints of Nevada. (See Appendix J-A-42-68) the P.U.C. wasting of time creating a paper chase.

Petitioner was trying to exhaust his remedies at law. The continuing behavior of parties that lack ethics and integrity of NRS procedures violates several of the petitioner's constitutional rights. Petitioner could file a complaint tomorrow (See Appendix R-A-227-242, S-A 243-253, W-A-289-293) with the P.U.C., and waste everybody's time and resources to run people in circles again, to have the same outcome to no adequate remedy of law and to have no resolution towards the problem. Due to lack of ethics needs for review of procedures, to protect consumers' rights that deal with State and Federal issues for proper due process. The lady of Justice is crying for help this is happening across the United States. It is time for the parties to cut their losses, stand up, and fight for our rights. This cancer that is taking over our businesses of Nevada deserves the proper discloser of information instead of pushing consumers in front of a truck for resolution of complaints. The financial burden and irreparable damages, to small business of today deserves a review of standards of procedures for deceptive, abuse of discretion in the State of Nevada.

CONCLUSION

For the forgoing reasons, the judgment of the Court of the appeals should be reversed and the case remanded with instructions to the District Court to review the procedures for P.U.C. decision. That has State and Federal issues presented to be fact by the P.U.C. Staff that ENDANGERS the PUBLIC and RISKS National Security at a time of War. While these acts towards the consumers lack integrity, the arbitrary and capricious acts were Blanton, deceptive acts towards the courts. The entire record from start to present shows the deceit by a monopoly of the State of Nevada that CONCEALS it security breaches and FAILED TO DISCLOSE was allowed to DESTROY RECORDS BY PERJURY.

A CORPORATION should not be Above the Law. The P.U.C. function is to resolve complaints and to protect the public interest the state agency has failed the public. All procedures need to be reviewed to better help serve the public .NRS statues need to revised, to catch up with technology and abuse of today. P.U.C. handling of over 50 complaints is just in one industry is (run and hide, close the door, be quiet they will be out of money soon, and go away. Complainants and Petitioner have lost everything including his family, due to organize crime issues. Petitioner spent over $500,000 in time and money since 1992. Petitioner has thousands of documents and expert testimony, that was generated of past and present access of SS7network events (See Appendix K-A-69-83). Bringing these issues that pledge our society at these times, due to rapid growth of our technology, law officials show P.U.C. CAN'T KEEP UP WITH cyber criminals of INLAND TERRORIST GROUPS having accessing to data basis, with personal information of networks. This makes the public at risk to identity theft (See Appendix T-A-276, X-A-309-341). Petitioner asks, if the FBI cannot protect its own lines than what is a consumer supposed to do? (See Appendix P-A-183). The

tariffs are no relief for the public tariffs are in favor of the Telco's. All other carriers ATT, MCI, QUEST long distance, LOCAL MGC etc. are all resellers of Sprint and tariffed to pay Sprint, for usage of cable facilities . Carriers being competition of Sprint, all have filed anti trust suits against, Sprint for blocking of their networks provided by Sprint. There again, the public is at the bottom of the chain, end-to-end guarantees are false hopes (See Appendix L-A-84-101).

The 30-day appeal was an escape door. That was untimely STATUE due to Federal issues of the hearing (See Appendix N-A-112-133, A-A-1-16) and amount of review transcripts, documents, testimony .hearing procedures, everybody took to hide behind. The District Court allowed Sprint's attorney to draft and order which was not consistent with the transcripts of 1-24-2005 (See Appendix Q-A-218-226). They should have recognized the USCA Title 47 ACT Telecommunications takes control over State issues presented. The bate and switch of proposed testing to Petitioner was another time delay of promises that were not kept due to threats to P.U.C. closed all efforts to find a resolution. The breaches of security Sprint is mandated to keep bell core standards mandated by the FCC. The intrastate and interstate federal jurisdiction preempts 800#'s of telephones' toll fraud which left the P.U.C. without the force of law (See Appendix J-A-42-68). P.U.C. knew that they did not have the expertise to check the integrity of a network or the resources (See Appendix X-A-294-339) to place the burden of proof on Petitioner were unreasonable for several reasons (See Appendix U-A-270-282). No access or recourses to check network petitioner is a consumer that pays for services. Petitioner is not a telephone company with the equipment or expertise, despite the fact that the petitioner managed to prove several incidents and brought forth several issues to the plate. Petitioner comes forth with petition of writ certiorari, as this is the last hope for the public to be treated fairly. Exhibits and records incorporated of appeal show the publics out cry for help. Petitioner respectfully submits the said writ of certiorari.

DECLARATION IN SUPPORT OF PETITION OF WRIT OF CERTIORARI

I, EDDIE PAUL MUNOZ, sworn under oath that said affidavit is true and correct to the best of my knowledge. I, EDDIE PAUL MUNOZ, since 1991 have been going thought the said statements pertaining to the lack of ethics and standards of procedures of facts and findings of criminal acts conducted by Sprint and the P.U.C. Their discretions toward the court were deceptive acts and they should have been held in contempt of court of petitioner's rights for judicial review of the P.U.C. As up to 2006, unfair business practices in Nevada are not in consumers and public issues of national security and are leaving Nevadans at risk. These crimes are spreading through the country at an alarming rate.

January 2, 2007
Sworn Under Chapter 52 Penalty of Perjury

(s)_____
EDDIE PAUL MUNOZ

NO._____

IN THE
SUPREME COURT OF THE UNITED STATES

EDDIE PAUL MUNOZ, PRO SE
PETITIONER

VS

CENTRAL TELEPHONE COMPANY
NEVADA; ET AL
RESPONDENTS

PROOF OF SERVICE

I, EDDIE PAUL MUNOZ, do swear or declare that on THIS DATE, MARCH 4, 2007, as required by SUPREME COURT RULE 29 I have served the enclosed MOTION for LEAVE to PROPER (pro se) PERSON and PETITION FOR A WRIT OF CERTIORARI AND JOINT APPENDIXES 1-5 on each party to the above proceeding or that parties consul, and on every other person required to be served , by depositing an envelope containing the above documents in the UNITED STATES mail properly addressed to each of them and with first-class postage prepaid or by delivery to a third -party commercial

carrier for delivery within 3 calendar days.

The names and addresses of those served are as follows;

PATRICK J. REILLY ESQ.
HALE LANE PEEK DENISON
AND HOWARD
3930 Howard Hughes Parkway
4th Floor
Las Vegas, NV 89109
TELEPHONE 702-222-2500

I declare under penalty of perjury that the foregoing is true and correct.

Executed on 3-4, 2007

(s) _____
EDDIE PAUL MUNOZ

APPENDIX A

Louise Uttinger, Esq.
Nevada State Bar No. 1971
PUBLIC UTILITIES COMMISSION OF NEVADA
1150 East William Street
Carson City, NV 89701
775/687-6002

BEFORE THE PUBLIC UTILITIES COMMISSION OF NEVADA

Eddie Munoz vs. Central Telephone Company Of Nevada, d/b/a Sprint of Nevada. Complaint Alleging incoming calls are being blocked or Diverted from customer's business.

_____/

Docket No. 00-6057

_____/

REGULATORY OPERATIONS STAFF'S POST-HEARING BRIEF

Regulatory Operations Staff ("Staff") of the Public Utilities Commission of Nevada ("Commission"), hereby submits its brief regarding Mr. Eddie Munoz' complaints of call diversion, call blocking, poor quality of service and lack of security on the Sprint (previously Central Telephone Company-Nevada, or "Centel") telephone system from the early 1990's to the present date.

Whether or not Mr. Munoz' business has experienced call blocking or call diversion is an issue that may be determined by the Commission in this case. Additionally, Mr. Munoz' current complaint[1] includes allegations that Nevada Sprint telephone system lacks

---

[1] October of 1999. Mr. Munoz' current complaint alleges that hotel calls are only received sporadically. Tr. At 276,ll. 1-4; 410, ll.16-24; Ex. 14.

security. Those allegations were supported by compelling, credible testimony from Mr. Munoz' expert witness, Mr. Kevin Mitnick, who testified that from 1993 to February of 1995[2], he could access any dial tone in Las Vegas, intercept calls and silently monitor any telephone line within the Las Vegas area through dial-up modems[3] associated with a testing system called the Centralized Automated Loop Reporting System (CALRS)[4]. Mr. Mitnick also testified that he had access to the local telephone system through the Nortel DMS100 switch.[5]

Although vast technological changes have occurred since 1995, Sprint's witness testimony in this record about its own security practices provides this commission with little or no assurance that the Nevada Sprint telephone system is secure. Mr. Munoz,[6] Mr. Mitnick[7] and public witness Stewart Nelkin[8] also believe that Sprint's security practices jeopardize national security.

The record demonstrates how little the Nevada Sprint is telling, even in general terms, about its most basic security practices and procedures. Evidence in the record from Sprint's own witness establishes that Sprint's switch log and data retention policies have prevented Sprint from systematically analyzing intrusion attempts and system vulnerabilities. While Staff concludes that numerous factors may be contributing to Mr. Munoz' service problems, this complaint has revealed significant

---

2 Tr. At 618, II.12-25. Mr, Mitnick recalled hacking Centel/Sprint "after December of '92." Id at 1.18.

3 Used by Northern Telecom, now Nortel Networks or "Nortel", to service the switches remotely.

4 Tr. At 798, II. 17-5; 799-803; 804, II. 1-3; 809, II 4-19; 811, II. 9-25; 812, II. 1-10. Ex. 43, Direct Testimony of Kevin Mitnick, Q & A 6.

5 Tr. At 804, II. 4-25; 805; 811, II. 9-25; 812, II. 1-10.Ex. 43, Direct Testimony of Kevin Mitnick, Q & A. 2,3, and 4.

6 Tr. at 426, II. 3-16. Mr. Munoz testified, "If they can do this to me, they can do this to Las Vegas." Id. At II. 5-6

7 Tr. at 612, II. 13-25; 613;614, II. 1-16. Ex. 45, p.3.

8 Tr. at 5[illegible] 5-15. Mr. Nelkin's testimony related to Sprint, Florida.

Sprint specific security issues that require prompt and thorough regulatory review.

I. Numerous Factors May Cause Mr. Munoz' Telephone Complaints

The Complainant in this case, Eddie Munoz, is the publisher of several adult advertising news rack papers[9] that promote in room entertainers, primarily in the Las Vegas area.[10] Mr. Munoz' publications advertise telephone numbers for adult entertainment businesses and individual entertainers; those advertised telephone numbers are supposed to ring to Mr. Munoz' business.

Mr. Munoz asserts that Sprint has allowed calls to his business, primarily from Las Vegas strip hotels,[11] to be diverted, blocked, or otherwise controlled or routed to competing outcall service businesses.[12] Mr. Munoz alleges that some callers to his business get false busy signals,[13] beeping sounds,[14] or dead air;[15] that calls are gone before they can be answered;[16] that phones cut off in the middle

---

9 Tr. at 176, II. 5-25; 117, II. 1-4; Tr. at 189, II. 9-15: 190, II. 1-13; 192, II. 10-25; 193, II. 1-8; 194, II. 7-25; 195, II. 1-13; 195, II. 22-25; 196; 197, II. 5-25; and 261, II. 1-13.

10 Tr. at 261, II. 12.

11 Ms. Maragret Munoz, receptionist and bookkeeper, estified that on the Sprint lines calls would come in from cell phones, local and long distance home phones, but few hotel calls ere received. Tr. at 160, II. 13-20; 167, II. 6-17; 205, II. 17-25; 206, II. 1-8. During the November 2000 test, Ms. Munoz testified that for the calls she ansered, only test calls ere received from hotels. Tr. at 222, II. 15-25; 223, II. 1-4. Mr. Munoz testified that the only hotel calls received during the test were from cell, house and pay phones. Tr. at 276; 277; 278, II. 1-6. See also Ex. 15, Staff's Data request 16.

12 Tr. at 220, II. 9-25; 221, II. 21-25; 222, II. 1-12.

13 Tr. at 293, II. 13-24; 347, II. 21-25; 348, II. 1-9.

14 Tr. at 159, II. 8-11. Ex. 6, Direct Testimony of Margaret Munoz, Question and Answer 7. Tr. at 206, II. 9-21.

15 Ms. Munoz testified that the line seemed to be open but no one was there. Ex. 6, Direct Testimony of Margaret Munoz, Question and Answer 5. Tr. at 156, II. 23-25; 157; 158, II. 1-16.

16 Tr. at 178, II. 18-25; 179, II. 1-7. Ms. Munoz also testified that real time data reports from AT&T shoed "That if calls were coming in from actual hotel numbers, that they were very short, like a 5-second period of time, because on the real-time data they would do it in increments of seconds." Tr. at 161, II. 10-18.

of conversations;[17] that his business phones stop ringing for extended periods during hours that normally are his busiest hours;[18] and that during such periods not even wrong numbers are received.[19] Cross talk or hearing a conversation on a line but not being able to talk to the person was also experienced.[20] Mr. Munoz and his employees record all phone calls on "What's Happening Logs".[21] Despite changes in providers, the problems persist.[22]

Public witnesses, including a Las Vegas attorney,[23] bail bondsmen[24] and a 24 hour adult phone line business owner[25] and Mr. Munoz' witnesses, including former outcall service operators[26] and a private investigator,[27] alleged similar problems each believed to be related to call diversion or blocking on the Sprint system.

The Commission received several similar complaints in the 1990's related to the Sprint (Centel)

---

17 Tr. at 159, II. 12-20.

18 Margaret Munoz testified that phone lines would go down for a couple of minutes to an hour; Ms. Munoz testified that she first observed phone lines going dead in May of 1997 and the problem continued to get worse. Tr. at 155, II. 5-25; 156, II. 1-8.

19 Tr. at 175, II 7-13.

20 Tr. at 438, II. 2-13.

21 Tr. at 151, II. 9-23; 299, II. 13-25; 300, II. 1-12. Mr. Munoz testified that all calls are counted and recorded on What's Happening Logs, including clicks, hang ups, and dead air. Id.

22 Tr. at 173, II. 21-25; 174; 175, II. 1-13. The AT&T test in one month in 1997 showed over 4,000 calls, with 677 unanswered; Mr. Munoz testified that those calls were not received. Tr. at 488, II. 18-25; 489, II. 1-18.

23 Tr. at 14-23.

24 Peter Vilencia and Johnny McDaniel, Tr. at 14-18.

25 Tr. at 589, II. 15-25; 590-598.

26 Ms. Hilda Brauer, Tr. at 59-98 and Mr. Lawrence Reubel; 102-147.

27 Mr. Heilman, Tr. 226-257.

telephone system,[28] including complaints from Ms. Brauer,[29] Mr. Reubel,[30] and Mr. Born.[31]

Mr. Munoz ordered his TI line from Sprint prior to the November 2000 testing, so that Sprint would be involved as both his local and long-distance phone company.[32] Prior to that test, Mr. Munoz had plain old telephone service ("POTS"). At the time of the hearing, Mr. Munoz' Sprint T1 line was disconnected,[33] leaving Mr. Munoz with POTS numbers.[34]

Test calls conducted to Mr. Munoz' business during selected hours on November 11, 14, and 18, 2000,[35] were received, with the exception of wrong numbers and numbers not ported correctly.[36] However, Mr. Munoz testified that during the test no calls from hotel rooms were received other than the test calls;[37] that Sprint's employees used cell phones during the test;[38] and that too many people knew about the test.[39]
Additional testing was performed by Mr. Munoz, who hired Alex Kasper and Kevin Mitnick; the Nexspace testing[40] introduced an entirely new system, lead to

---

28 Tr. at 814, II. 24-25; 815, II. 1-10; 823, II. 10-25; 824; 825, II. 1-5; Tr. at 819, II. 11-22; Ex. 54. Staff received both written and telephone complaints. Tr. at 849, II. 19-25; 850, II. 1-15.

29 Tr. at 63, II. 24-25; 64-70. Mr. Heilman worked for Mr. Born. Tr. at 69, 1. 25; 70, II.1-2.

30 See Ex. 5 and Tr. at 104, II. 10-25;105-106;107, II. 1-18.

31 See Ex. 3 and Tr. at 228, II. 1-18. Mr. Heilman worked for Mr. Born and investigated the Brauer complaint, but not the Born complaint. Tr. at 228, II. 1-18.

32 Tr. at 266, II. 1-5; see also 727, II.21-25; 728, II. 1-4; 264, II. 2-4.

33 Tr. at 315, II. 17-23;263, II. 21-25; 264, 1.1.

34 Mr Collins agreed that call forwarding could be added to POTS numbers, but not the Sprint T1 line. Tr. at 745, II. 17-25; 746; 747, II. 1-2. When testifying about the "number Mr. Munozhas", Mr. Collins as referring to the T1 numbers that Mr. Munoz ordered for the Sprint testing. Id.

35 Tr. at 273, II. 6-14.

36 Tr. at 552, II. 14-25; 553-561; Ex.41;Ex. 26.

37 Tr. at 276, II. 22-24; 277, II. 5-7.

38 Mr. Collins confirmed that cell phones were used. Tr. at 736, II. 12-22.

39 Tr. at 456, II. 22-24; 462, II.9-16.

40 Tr. at 265, II. 2-25; 266; 267; 268, II. 1-9.

expected difficulties in introducing a new system and did not shed any light on Munoz complaint.[41]

Mr Mitnick's prefiled[42] and direct testimony asserted that he had complete access to all of Centel's (Sprint's) phone lines. Mr. Collins attempted unsuccessfully to minimize Mr. Mitnick's prior access to the local telephone system, stating: "...the allegations that Mr. Mitnick made were for plain old telephone service compared to Mr. Munoz' service which is a different type of service."[43] While that statement is only true for the Munoz Sprint T1 line,[44] the record contains no evidence that T1 service is more or less secure than any other service.

Mr. Munoz' refusal to maintain or update the WIN-100D, a critical part of his business infrastructure,[45] limits the primary documentation of his complaint to hand written calling logs. Staff and Mr. Munoz's prior consultant find these logs an inadequate basis to support Mr. Munoz' claims of service problems.[46] Staff would suggest that Mr. Munoz update his PBX and begin using one of the many low cost software packages available to refine his recordkeeping. This would eliminate the problem of comparing Sprint and Munoz records (the issue of time synchronization) and many sources of human error. A controlling software package would allow Mr. Munoz to quickly verify the status of all incoming lines, and provide sufficient documentation to substantiate his service complaints as to when those lines are out of service.

In order to eliminate all of the allegations made in this case, careful, simultaneous testing on both ends of the

---

41 Tr. at 638, ll. 9-25; 639, ll. 1-4.

42 Ex. 14, 60 and 61.

43 Tr. at 712, ll. 2-5.

44 Mr. Collins agreed that Mr. Munoz'. Sprint T1 line was ordered, set up and serviced by Sprint Long Distance. Tr. at 714, ll. 21-25; 715, ll. 1-4. He also confirmed that the Sprint T1 line did not support call forwarding. Tr. at 717, ll. 9-17.

45 Tr. at 282, ll. 7-25; 283, ll. 1-21.

46 Ex. 40, Feb. 17, 1997, at 2, 4(c), second paragraph-end. Tr. at 542, ll. 11-25; 543, ll. 1-3.

DMS100 to Mr. Munoz link was required.[47] Records of that testing should have been kept for review by the Commission and Staff. In the absence of such testing and records, Staff concludes that numerous factors may contribute to Mr. Munoz' service complaints; while the Sprint telephone system cannot be ruled out as a contributing factor, neither can it be determined to be solely responsible.

II. Sprint's Security Procedures Require Additional Regulatory Review.

back door n. In the security of a system, a hole deliberately left in place by designers or maintainers. May be intended for use by service technicians.

security through obscurity (alt. security by obscurity) A hacker term for vendors' favorite way of coping with security holes – namely, ignoring them; documenting neither any known holes nor the underlying security algorithms; or trusting that nobody will find out about them, and that people who did find about them won't exploit them. This "strategy" never works for long.[48]

Throughout this case, Sprint steadfastly denied that its telephone system had ever been penetrated. If Sprint's telephone system has been penetrated, the Company represents that it does not know it.[49] Sprint's corporate denial was reaffirmed by Mr. Collins on June 24, 2002, immediately after Mr. Munoz' witness, Mr. Kevin Mitnick, testified to accessing the local Sprint/Centel telephone system.

While Staff does not doubt that Sprint does not know if its telephone system has been compromised or penetrated, Sprint's investigation of Staff's inquiry appears to be quite limited. In order to respond to Staff's

---

47 That testing was not performed.

48 Adapted from *The New Hacker's Dictionary* (MIT Press) by permission of Eric S. Raymond

49 Tr. at 710, II. 1-20.

Data Request No. 8, Mr. Collins testified that he asked fellow Sprint employees if they were aware of system penetrations.[50] However, Sprint provided no evidence regarding what analyses ere performed.

During the hearing, Sprint provided no evidence that the company monitored its switches or took other affirmative security measures in order to determine if its telephone system was secure. Sprint could have automated downloading and analysis of all switch log data to detect intrusions, but apparently did not. Mr. Collins testified that only a portion of Sprint's switch log data as kept for less than 48 hours,[51] an insufficient time period for any analysis of prolonged or repeated intrusion attempts, assuming that Sprint performed such an analysis.

Sprint's regulatory witness[52] denied that Sprint had knowledge of any intrusion or penetration of its telephone system,[53] yet claimed that Sprint made unspecified improvements in its system security to prevent the type of access described by Mr. Mitnick.[54] Mr. Collins' testimony regarding when Sprint made security improvements was vague,[55] as were his responses to questions asking what persons or groups were responsible for new Sprint switch security procedures.[56] Mr. Collins did not know when unspecified improvements were made[57] and claimed "...it's been an ongoing process since approximately 1996,1997."[58]

---

50 Tr. at 710, II. 19-25; 711, II. 1-8. *See also* Tr. at 712, II. 11-24; Ex. 49, Staff Data Request No. 8.

51 Tr. at 792, II. 13-25.

52 Mr. Collins confirmed he was not a technical witness. Tr. at 698, II. 23-25; 697, II. 1; 561, II. 13-19.

53 Ex. 49, Staff Data Request No. 8; Tr at 710, II. 6-25; 711; 712, II. 1-24. Sprint's claim does not distinguish between the type of telephone service received. Tr. at 712, II. 6-10. Mr. Collins testified that he made the claim as Sprint's representative of the investigation. Tr. at 765, II. 14-25; 766, II. 1-4. Collins also testified that his testimony had not been contradicted by "anyone within Sprint". Id.

54 Tr. at 704, II. 23-25; 705, II. 1-3.

55 Tr. at 705, II. 6-24.

56 Tr. at 706, II. 8-22.

57 Tr. at 704, II. 5-10; 704, II. 23-25; 705, II. 1-24

58 Tr. at 705, II. 21-24.

Significantly, Sprint offered no documentary evidence or technical witness who could confirm what security procedures the company had implemented to assure the Commission that the Nevada Sprint system presently is secure.[59] Similarly, Sprint presented no technical witness who was knowledgeable about either the Munoz complaint or Sprint's present telephone system security practices.

Sprint also failed to establish what security procedures are in place to protect its telephone system from the types of intrusions alleged by Mr, Munoz[60] and testified to by Mr. Mitnick; Sprint offered no evidence that it could currently prevent the ready access Mr. Mitnick detailed through either the DMS100 switch or the CALRS system.

Sprint's witness, Mr. Scott Collins, confirmed a lack of Sprint employee "social engineering"[61] security training.[62] He discounted Mr. Mitnick's testimony, saying "He just don't (sic) call up and ask for it. He conned his way in as either posing as a fellow Sprint employee or Nortel technician".[63] However, calling up and asking for information is precisely what social engineering entails.

Mr. Collins also testified that Sprint's telephone switch logs were maintained for approximately a two-day period.[64] While Sprint now might be retaining switch log

---

59 Sprint could have provided a technical witness regarding any of its security practices that would present the types of access alleged by Mr. Munoz and testified to by Mr. Mitnick. It did not do so. Sprint's security testimony and any documents claimed to be confidential could have been filed under seal with the Commission and a closed hearing held. Sprint elected not to do so.

60 Tr. at 814, II. 8-12. Mr. Hackman offered no opinion as to whether any of Mr. Munoz's calls are being blocked or diverted.

61 Mr. Mitnick further defined social engineering. See Tr. at 602, II. 16-25; 603, II. 1-3.

62 Tr. at 707, II. 9-11; 708, II. 10-25; 709, II. 1-17. Mr. Collins testified that Sprint's employees are trained to protect customer propriety information. Tr. at 707, II. 12-18.

63 Tr. at 709, II. 6-10.

64 Tr. at 719, II. 12-25; 720, II. 1-14. Ex. 51, Staff's Data Request 32 requested that Sprint provide "... copies of any and all logs kept for switch access obtained via interanal modem lines for the last seven years." None were provided by Sprint. Id. at 720, II. 12-21.

data for a longer period,[65] Mr. Collins did not know if in fact Sprint reviewed switch logs for intrusion attempts.[66] Mr. Collins also informed Commission Policy Advisor Mr. Bolle that he did not know whether or not Sprint downloaded data from the switch logs:

Q. With respect to the dial-up access log, is it my understanding that that log is kept for 48 hours; id that right?

A. It's my understanding that a log for dial-up access into the switch is kept for 48 hours, or there's a certain amount of data I believe that's held and then it's rewritten. And I believe it approximates the 48 hours.

Q. What happens to that report in that 48 hours, do you know?

A. I believe we are – and I'm not sure, but I believe we now maintain that in a database somewhere. I don't know if that was always the policy.[67]

The limited data Sprint briefly kept may not have been retained solely or primarily for security purposes. Sprint may have maintained dial-up[68] data solely for billing purposes. While Sprint's response to Staff Data Request 32, Exhibit 51, states that only dial-up or remote access activity was kept for "approximately two days", it is unclear what, if anything, Sprint did with the data it briefly retained.

---

65 Mr. Collins testified that switch logs are "...kept for a cerain amount of time." Tr. at 766, ll. 11-19.

66 Id.

67 Tr. at 792, ll. 13-25. Emphasis added. Since he responded to Staff's Data Request 32 and 38, Ex. 51, Mr. Collins did know that as of November 30, 2001, switch log dial-up or remote access data was not retained for more than two days. Mr. Collins represented in response to Staff's Data Request 32 that "Logs showing dial-up or remote access activity into Sprint's Las Vegas switches are kept for approximately two days. Sprint is therefore unable to provide these logs for the past seven years."

68 Newton's Telecom Dictionary, 17th edition, defines "Dial Up": "the use of a dial or push button telephone to create a telephone or data call. Dial up calls are usually billed by time of day, duration of call and distance traveled. A connection to the Internet, or any network, where a modem and a standard telephone are use to make a connection between computers. See Dial Up Line."

Assuming, *arguendo*, that Sprint's employees promptly reviewed this limited switch log data for security purposes before it was overwritten, Sprint nevertheless did not retain switch data by which it might identify a pattern of attempted system intrusions through its switches. If Sprint automatically downloaded data for analysis and retention, Sprint could answer critical questions, including when a system intrusion took place, thereby identifying the period of exposure; how access was gained; what information was compromised; and how similar access could be prevented.

While several questions still exist concerning Mr. Munoz' business practices and customer premises equipment ("CPE"), Sprint's business practices and its response to this complaint fail to provide evidence that the Sprint of Nevada's telephone system is presently secure.

Sprint did not maintain or produce copies of its investigative files or reports for Mr. Munoz' complaints or similar complaints of call blocking or call diversion investigated by Mr. Hill and Mr. Poole.[69] Mr. Collins testified that Sprint's record retention policies varied by department.[70] Investigative records or reports related to the Munoz investigation were either not produced[71] or were destroyed in a re-organization.[72] Absent written reports, Mr. Collins agreed that Sprint would have to rely on its employees' institutional knowledge and involvement in the test or investigation.[73] However, the Sprint employee produced as a witness in this case who investigated complaints could not specifically recall working on the Munoz complaint.[74]

Sprint's failure to produce a technical witness familiar with Sprint's current security practices and policies gives Staff no comfort that Sprint has in place

---

69 Tr. at 385, ll. 8-14; Tr. at 752, ll. 5-25; 753; 754, ll. 1-7.

70 Tr. at 754, ll. 8-25; 755, ll. 1-24.

71 Tr. at 752, ll. 17-25; 753, ll. 1-3.

72 Tr. at 753, ll. 23-25; 754, ll. 1-7.

73 Tr. at 753, ll. 17-22.

74 Tr. at 383, ll. 14-16. Mr. Hill also testified that he maintained personal investigation records but did not know where the records went after he left Sprint. Tr. at 385, ll. 8-14.

either adequate security protocols or sufficient employee security training. Whether or not the Commission determines that Mr. Munoz' business calls were subject to call diversion or call blocking, based on the record and evidence in this case, the Commission should find that an unreasonable opportunity for call diversion or call blocking exists on the Sprint Nevada system.

Accordingly, the Commission should enter an Order that adopts Staff's recommendations[75] and requires Sprint to retain outside consultants to conduct a Staff monitored internal Sprint security review. The Commission should also establish subsequent security reporting requirements to ensure that Sprint will create and maintain adequate security protections and investigative records retention policies. Sprint also should demonstrate that its employees are trained to follow Sprint's security practices and records retention policies. Local Sprint employees, Sprint corporate, and any other Sprint employees who have any shared responsibility for the security of the Nevada Sprint telephone system should be included in Sprint's security training.

III. Security of Telephone Service Is Jurisdictional to the Commission

Mr. Munoz presents this Commission with a critical issue: Is the telephone service provided by Sprint in its Nevada service territory secure? The answer to that question could impact economic, social, and national matters of importance to all Nevadans and to anyone conducting business in Nevada. Mr. Munoz asserts that Sprint has not adequately protected its customers from security breaches that have occurred and has not done adequate and proper testing of Sprint's telephone system.[76]

Moreover, Sprint clearly was aware of customer complaints alleging diverted or blocked calls from the 1990's to date. Sprint also knew of alleged access through CALRS at least since the time Mr. Mitnick filed testimony

---

[75] Ex. 7, Direct Testimony of Ron Bardarson, at 10, ll. 16-21.

[76] Ex. 60, 4A.

in this case. If Mr. Mitnick's testimony related to the asserted password seed list[77] is correct,[78] Sprint may have failed to timely change Nortel's pre-programmed passwords to protect Sprint's telephone system. Moreover, Sprint provided no evidence to establish when or if the Nortel passwords had been changed, or if such asserted access was no longer possible.

Based on Staff's investigation and evidence in the case, Staff recommends that Sprint review its security procedures throughout its Nevada telephone system. Staff also asks the Commission to order Sprint to retain telephone security consultants to advise the Company of additional security measures that may be warranted; to prevent or deter access to Sprint's Nevada telephone system, including telephone switches; to train its employees to detect and deter intrusion attempts; to automate an iterative process to precisely identify and contain telephone system intrusions; and to document ad record its Nevada security investigations.

Staff's security recommendations are timely.[79] Adequate telecommunication security is an ongoing, ordinary part of doing business. The security of a telephone call is directly related to the service rendered by Sprint in accordance with tariffs filed with and approved by the Commission.[80] Similarly, the quality of service

---

77 Ex. 52.

78 Tr. at 798, II. 17-25; 799; Ex. 43.

79 The Federal Energy Regualtory Commission (FERC) and North American Electric Reliability Council (NERC) recently identified a set of "Minimum Dailily Security Requirements" to be included in the Notice of Proposed Rulemaking for Security Standards for the Electricity Sector, july 19, 2002. The Primary Focus is on Cyber Security, including physical security of cyber assets.

80 NRS 703.150 gives the Commission the authority to supervise and regulate the operation and mainteneacnce of public utilities in this state; NRS 704.120 gives the Commission the authority to substitute such rates, regulations, practices, or service after investigation and hearing as is just and reasonable.

rendered by Sprint is clearly within this Commission's jurisdiction.[81]

CONCLUSION

Mr. Hackman described his levels of faith in Sprint's investigation as being "somewhat like a roller-coaster ride"; he had less faith in the thoroughness of the Company's investigations that were done in the mid-1990's, but more faith in the thoroughness of the Company's investigation and level of attention given to the case in the last two to three years.[82] Mr. Hackman stated that:

> "I believe that Mr. Munoz is experiencing the problems that he described. I just have not seen enough compelling evidence to conclude that Sprint is the cause of it".[83]

Mr. Bardarson's review of the complaint and the record in this case discloses a variety of potential causes of Mr. Munoz' telephone problems. The Munoz and Sprint ends of the calling chain, as well as the transmission portion of the call are suspect.

Staff therefore recommends that the Munoz complaint be dismissed and that the Commission order Sprint to retain outside consultants to conduct a comprehensive security review of Sprint's Nevada operations. Staff respectfully requests that the Commission enter and Order that:

1. Dismisses the Munoz complaint and adopts Staff's recommendations[84] and

2. Orders that a new Commission investigagoy docket be opened immediately to investigate Sprint's Nevada security, security practices, and employee security training and

3. Requires:

---

81 NRS 704.001.

82 Tr. at 847, ll. 11-24.

83 Tr. at 855, ll. 14-17. *Also see* Ex. 53, the Direct Testimony of Rick Hackman.

84 Ex. 7, Direct Testimony of Ron Bardarson, at 10, ll. 16-21.

a. Sprint and its corporate security representatives to meet with Staff within 15 days of an Interim or Final Commission Opinion and Order in Docket No. 00-6057 and subsequently, when Sprint's consultants have been retained, to coöperatively develop and implement a schedule for a comprehensive Sprint Nevada security review conducted by consultants for Sprint and monitored by Staff, and

b. Sprint to utilize consultants to modify Sprint's local and corporate security practices and procedures related to its Nevada operations:

1) to maintain and protect Sprint's Nevada confidential corporate information;

2) to prevent or deter access to Sprint's Nevada telephone system, including its Nevada telephone switches;

3) to developed and automate systems to identify attempted Nevada telephone system intrusions;

4) to develop ad implement mandatory employee reports, logs and records retention policies for documentation of its Nevada security investigations and

5) to develop and conduct a Nevada Sprint employee security training program, monitored by Staff, including training in specific techniques to better maintain confidential corporate information; methods to prevent or deter access to Sprint's electronic systems; and procedures to encourage employee recognition, identification and reporting of social engineering or "con" attempts and

6) to conduct active testing to ensure that any adopted changes are implemented and effective.

4. Require Sprint, in consultation with its consultants, and Staff to propose to the Commission an issue specific investigatory schedule, including time frames for completion, periodic reporting requirements and Commission hearings, including time frames for

completion, periodic reporting requirements and Commission hearings, including closed hearings, and

5. Specifies that any information related to the Munoz complaint that may be discovered in a subsequent investigatory docket be filed with the Commission and be provided to counsel for Mr. Munoz and Staff; if any such information relates to a Sprint security practice currently used with Sprint, such filing may be made under seal with the Commission and provided by Protective Agreement to counsel for Mr. Munoz and Staff, the parties to Docket No. 00-6057.

RESPECTFULLY SUBMITTED this 16th day of August 2002.

PUBLIC UTILITIES
COMMISSION OF NEVADA
REGULATORY OPERATIONS
STAFF.

By: (s)
Louise Uttinger,
Assistant Staff Counsel

APPENDIX B

Louise Uttinger, Esq.
Nevada State Bar No. 1971
PUBLIC UTILITIES COMMISSION OF NEVADA
1150 East William Street
Carson City, NV 89701
775/687-6002

BEFORE THE PUBLIC UTILITIES COMMISSION OF NEVADA

Eddie Munoz vs. Central Telephone Company Of Nevada, d/b/a Sprint of Nevada. Complaint Alleging incoming calls are being blocked or Diverted from customer's business.

_____/

Docket No. 00-6057

_____/

REGULATORY OPERATIONS STAFF'S MOTION TO DESIGNATE CONFIDENTIAL INFORMATION AND MOTION TO ISSUE PROTECTIVE ORDER

COMES NOW, the Regulatory Operations Staff ("Staff") of the Public Utilities Cmmission of Nevada ("Commission") and, pursuant to Nevada Administrative Code ("NAC") 703.550, hereby submits its Motion to Designate Confidential Information and Motion to Issue Protective Order in the above-captioned docket. Staff's Motions are necessitated by a careful review of certain records filed in the open record in this case, including personal telephone numbers of customer who may have unlisted or non-published number or other reasonable expectations of privacy.

I. POINTS AND AUTHORITIES

NRS 703.190 (2) mandates that the Commission prohibit the disclosure of trade secret or confidential

commercial information pursuant to NRS 49.325 or NRS 600A.070 or Rule 26 (c)(7) of the Nevada Rules of Civil Procedure ("NRCP"). Nevada Rules of Civil Procedure 26 (c)(7) allows the issuance of protective orders, for good cause shown, for trade secrets and other confidential commercial information; additionally NRCP 26(c)(8) allows protective orders to require that certain information be filed under seal, to be opened as directed by the court.

> ...[T]he court in which the action is pending may make any order which justice requires to protect a party or person from annoyance, embarrassment, oppression or undue burden or expense, including one or more of the following:....NRCP 26(c).

Pursuant to NRCP 26(c), Staff's Motions seek to protect specific individual names and telephone numbers from being placed in the public record I this proceeding. Staff requests that the period during which the information must not be disclosed publicly by indefinite, until such time that all appeals in the case have been completed. At the conclusion of all appeals of any orders in this case, Staff requests that the Protective Orderspecify that such materials that exist in the Commission and Staff files be destroyed.

Chapter 703 of the Nevada Administrative Code sets forth the rules of practice and procedure before the Commission. Sections 703.527 through 703.5282, entitled "Confidentiality of Information", resulted from the regulations adopted in Docket No. 95-1016. These sections address the procedures for handling information deemed confidential or obtained under a protective agreement.

If granted, Staff's Motions would allow redacted volumes of information to be utilized at hearing, and would designate as confidential the Commission's copies of volumes of information currently available in the public record. To the extent that any injury is required into such designated confidential information during the course of the hearing, the Presiding Officer may close the hearing

and restrict persons present to counsel and their parties, excluding all others from the hearing room.

Due to the fact that the confidential information is interspersed throughout voluminous information, Staff provides one redacted set of materials to the Commission; Staff further represents that it previously provided one propesed redacted set to counsel for each party to the case. Staff, therefore, requests waiver of NAC 703.5274(1)(b), which would require 10 copies of the document which redacts the confidential information for which the confidential treatment is requested.

Attached to this filing are redacted copies of Volumes 1, 2 and 3 filed with the Commission on March 7, 2001.

RESPECTFULLY SUBMITTED this 31st day of October 2001.

PUBLIC UTILITIES COMMISSION OF NEVADA REGULATORY OPERATIONS STAFF

By: (s) _____

Louise Uttinger, Assistant Staff Counsel

APPENDIX C

BEFORE THE PUBLIC UTILITIES COMMISSION OF NEVADA

EDDIE MUNOZ vs. CENTRAL TELEPHONE COMPANY- NEVADA, d/b/a SPRINT OF NEVADA. Complaint alleging incoming calls are being blocked or Diverted from customer's business.

_____/

Docket No. 00-6057

_____/

INTERIM ORDER DENYING MOTION FOR PROTECTIVE ORDER AND DENYING MOTION TO COMPEL

The Presiding Officer in this docket makes the following findings of fact and conclusions of law:

1. A Complaint, designated as Docket No. 00-6057, has been filed with the Public Utilities Commission of Nevada ("Commission") by Eddie Munoz ("Complainant") against Central Telephone Company-Nevada, d/b/a Sprint of Nevada ("Sprint") in which Complainant alleged that incoming calls to his business in Las Vegas, Nevada, were either being blocked or diverted to another source within the Sprint network. Complainant requested an investigation and public hearing into the matter. On February 22, 2001, the Commission voted to set this matter for investigation and hearing.

2. This Complaint as filed pursuant to Chapters 703 and 704 of the Nevada Revised Statutes ("NRS") and Nevada Administrative Code ("NAC") and including but not limited to NRS 703.310.

3. The Commission issued a public notice of this Complaint in accordance with State law and the Commission's rules of Practice and Procedure.

4. On April 30, 2001, the Commission held a duly noticed prehearing conference regarding these matters.

5. On March 6, 2002, the Complaint filed a Motion for Protective Order ("Motion"). The Complaint asserted that the Motion is necessitated by the fact that two officers with the Las Vegas Metropolitan Police Department ("Metro") have agreed to discuss an ongoing investigation regarding call diversion which may be relevant to the instant case. The Complainant stated that the officers will comment during the public comments portion of the hearing scheduled for March 14, 2002, but only if such comments can be made in a closed session.

6. On March 8, 2002, Sprint filed its Opposition to the Motion ("Opposition").Sprint argued *inter alia* that the Motion is an attempt to introduce surprise testimony, which violates Sprint's Due Process rights to prepare for hearing.

7. On March 11, 2002, Complainant filed his Reply to Sprint's Opposition. The Complainant stated that Sprint "apparently misconstrued" the Motion.[1] The Complainant asserted that "it is Metro that is seeking an opportunity to share any relevant information with the Commission and not (Complainant) seeking to offer additional testimony."[2] The Complainant further stated that the comments are "not intended to be a question and answer session, but rather input which the public is entitled to have into a particular docket with the proviso that it be in a closed session...."[3] Also on March 11, 2002, Staff filed its Response to the Motion. Staff did not oppose the Motion to allow Metro to provide either testimony or comments in a closed session. Staff, however, requested several conditions that it would like to

---

[1] Reply to Sprint's Opposition to Motion for Protective Order at pg. 1

[2] *Id.*

[3] *Id.*

see present in the commission interim order granting the Motion.[4]

8. On March 13, 2002, Complainant filed a Motion to Compel Witnesses ("Motion to Compel"). The Complainant asserted that the Motion to Compel is necessary because the Metro officers cannot attend the hearing without a subpoena or a Commission order compelling them to appear.

9. On March 14, 2002, the Clark County District Attorney ("DA") filed a letter on behalf of Metro indicating its opposition to any order directing Metro representatives to testify regarding a confidential law enforcement investigation.

10. NAC 703.700 provides that "the presiding officer shall, upon... his own initiative... quash... the order "granting a motion for order to compel witnesses "if it is determined to be unreasonable or oppressive."

11. The Presiding Officer finds that if an order were issued granting to Motion to Compel, the order would be unreasonable in violation of NAC 703.700. Furthermore, to close a hearing during the public comment period of the hearing would violate the spirit, if not the letter, of the Open Meeting Law, NRS Chapter 241.

12. The Presiding Officer finds that Complainant's attorney has no standing to represent Metro, and thus does not have the capacity to request a Motion for Protective Order on Metro's behalf, a fact implicit in the filing of the Motion to Compel.

13. The Presiding Officer finds that the DA does have standing to represent Metro. The letter filed by the DA on March 14, 2002, stated that Metro Regulation 4/108.07 prohibits members from voluntarily testifying in civil actions, or testifying without being under subpoena. The letter further stated that Metro would move to quash any subpoena which was issued.

---

[4] Regulatory Operations Staff's Response to Munoz Motion for Protective Order at pg. 2.

14. Therefore, the Presiding Officer finds good cause to deny the Motion for Protective Order and the Motion to Compel.

15. Pursuant to NAC 703.690, the Presiding Officer may issue appropriate interim orders.

THEREFORE, it is ORDERED that:

1. The Motion for Protective Order filed in Docket No. 00-6057 is DENIED.

2. The Motion to Compel filed in Docket No. 00-6057 is DENIED.

3. The Commission retains jurisdiction for the purpose of correcting any errors that may have occurred in the drafting or issuance of the Order.

By the Commission,

(s)

ADRIANA ESCOBAR CHANOS, Commissioner and Presiding Officer

Attest: (s)

CRYSTAL JACKSON, Commission Secretary

Dated: Carson City, Nevada

(SEAL) 4-1-02

APPENDIX D

BEFORE THE PUBLIC UTILITIES COMMISSION OF NEVADA

EDDIE MUNOZ V. CENTRAL TELEPHONE COMPANY-NEVADA, d/b/a SPRINT OF NEVADA. Complaint alleging incoming calls are being blocked or diverted from customer's business.

Docket No. 00-6057

At a general session of the Public Utilities Commission of Nevada, held at its offices on September 12, 2002.

PRESENT: Chairman Donald L. Soderberg
Commissioner Richard M. McIntyre
Commissioner Adriana Escobar Chanos
Commission Secretary Crystal Jackson

ORDER

The Public Utilities Commission of Nevada ("Commission") makes the following findings of fact and conclusions of law:

1. A complaint, designated as Docket No. 00-6057, was filed with the Commission by Eddie Munoz ("Complainant") against Central Telephone Company-Nevada d/b/a Sprint of Nevada ("Sprint") in which Complainant alleged that incoming calls to his business in Las Vegas, Nevada ere either being blocked or diverted to another source within the Sprint network. Complainant requested an investigation and public hearing into the

matter. On February 22, 2001, the Commission voted to set this matter for investigation and hearing.

2. This complaint was filed pursuant to Chapters 703 and 704 of the Nevada Revised Statutes ("NRS") and Nevada Administrative Code and, in particular, NRS 703.310.

3. The Commission issued a public notice of this complaint in accordance with State law and the commission's rules of Practice and Procedure.

4. The Regulatory operations Staff of the Commission participated as a matter of right. The petitions for leave to intervene filed by Hilda Brauer, Larry Duke Reubel, Nicole Hamrah, and Stephanie Mouton were denied. Members of the public were given an opportunity to comment at the commencement of the hearing and at other times during the process as well.

5. On April 30, 2001, the Commission held a duly noticed prehearing conference regarding these matters.

6. On May 2, 2001, a Notice of Hearing was issued, establishing September 24, 2001 as the hearing date.

7. A Procedural Order was issued on May 15, 2001, establishing a procedural schedule in Docket No. 00-6057.

8. On July 26, 2001, Procedural Order No. 2 was issued. Also on July 26, 2001, the Presiding Officer issued an Order Granting Complainant's Motion to Extend Discovery and Continue the Hearing Date as well as an Order Denying a Countermotion filed by Sprint.

9. On December 24, 2001, an Order was issued Granting Staff's Motion to Designate Confidential Information and Motion to Issue Protective Order

10. On February 12, 2002, Procedural Order No. 3 was issued.

11. On March 7, 2002, an Order was issued Granting a Motion for Expedited Ruling and Denying All Other Pending Motions.

12. On March 14, 2002, a duly-noticed hearing was commenced.

COMMISSION DISCUSSION

13. The Commission addressed two issues during this proceeding. The issues are (1) whether call diversion and/or call blockage caused by Sprint has occurred and (2) whether Sprint has taken the necessary precautions to insure the security of its network.

14. As to the first issue of call diversion and/or call blockage, the record does not present evidence that Sprint has caused either to occur. In fact, Complainant's witness Kevin Mitnick testified that neither Nexspace nor himself could find any case where they could recreate the situation where a call was diverted to a competitor. (TRS Pg. 629; lines 17 through 22). Mr. Mitnick also testified that it was his opinion that further testing needs to be done. (TRS Pg. 657, lines 12 through 23). Mr. Mitnick further testified that he does not know if Mr. Munoz's calls are being blocked or diverted. (TRS Pg. 658, lines 15 through 24). Further, the record presents evidence that other causes may be responsible for Complainant's problems. These possible causes include but are not limited to the following: (1) Diversion and/or blockage of telephone calls at private hotel PBX systems (TRSPg. 641 lines 8 through 15), (TRS Pg. 854 lines 17 through 21); and (2) Complainants own equipment failure (Exhibit 31 Pg. 08359, para. C(4)(d)), (Exhibit 7 Pg. 5 lines 18 through 19), and (TRS Pg. 861 lines 8 through 10). These possible causes are not the responsibility of Sprint.

15. The Complainant must present sufficient evidence to support his allegations against Sprint. In this instance, the Complainant has not presented substantial evidence that call diversion and/or call blockage as caused by Sprint. Therefore, the Commission finds that the complaint alleging call diversion and/or call blockage should be dismissed.

16. As to the second issue, the record does not present sufficient evidence that Sprint has failed to take the necessary precautions to insure the security of its network.

17. Mr. Mitnick testified that any system that is controlled by computer systems is essentially

vulnerable. (TRS Pg. 613 lines 4 through 6). Mr. Mitnick also testified that he has compromised the networks of every telephone company in all the areas he was living while avoiding the government. (TRS Pg. 619 lines 12 through 21).

18. In fact, the record supports that Sprint has taken reasonable steps to protect its network. (TRS Pg. 651 lies 3 through 6), (Exhibit 7 Pg. 3 line 29), and (Exhibit 18 Pg. 7 lines 23 through 24). The record further supports that Sprint's network security is no better nor no worse than that of other telephone companies.

19. Again, the Commission expects the complainant to put forth sufficient evidence to support the complaint. The Commission does not find substantial evidence oj the record to support the complaint that Sprint has not taken reasonable steps to protect the security of its network. Therefore, the Commission finds that it should dismiss the complaint.

THEREFORE, it is ORDERED that:

1. The complaint filed by Eddie Munoz in Docket no. 00-6057 is dismissed.

2. All arguments of the parties raised in the proceedings, including but not limited to arguments raised in the hearing, not expressly considered herein have been considered and either rejected or found to be non-essential further support for this Order.

3. The Commission retains jurisdiction for the purpose of correcting any errors which may have occurred in the drafting or issuance of this Order.

/
/
/
/
/
/
/
/
/
/
/

By the Commission,

/s/
DONALD L. SODERBERG, Chairman

/s/
RICHARD M. MCINTIRE, Commissioner

/s/
ADRIANA ESCOBAR CHANOS,
Commissioner and Presiding Officer

Attest: /s/
CRYSTAL JACKSON, Commission Secretary
Dated: Carson City, Nevada
(SEAL) 9/23/02

APPENDIX E

Patrick J. Reilly, Esq.
Nevada Bar No. 6103
Thomas R. Ryan, Esq.
Nevada Bar No. 8647
Hale Lane Peek Dennison and Howard
2300 West Sahara Avenue
8th Floor, Box 8
Las Vegas, Nevada 89102
Telephone (702)222-2500
Facsimile (702)365-6940
preilly@halelane.com

Attorneys for Defendant

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

EDDIE PAUL MUNOZ,
Plaintiff,
vs.
CENTRAL TELEPHONE CO. NEVADA
d/b/a SPRINT OF NEVADA,
Defendant.
_____/
Case No. CV-S-04-1212-RCJ-RJJ

ORDER GRANTING DEFENDANT'S MOTION TO DISMISS WITH PREJUDICE
_____/

On January 24, 2005, this court heard oral argument on a Motion to Dismiss filed by Defendant Central Telephone Company – Nevada dba Sprint of Nevada ("Sprint") in the above-entitled action. Plaintiff Eddie Paul Munoz ("Mr. Munoz") appeared in proper person. Patrick J. Reilly, Esq.

of the law firm of Hale Lane Peek Dennison and Howard appeared on behalf of Sprint. After carefully considering the arguments and briefs of the parties, this Court hereby GRANTS Sprint's Motion to Dismiss.

I.
MUNOZ'S ALLEGATIONS[1]

1. Mr. Munoz operates an adult entertainment business located in Las Vegas, Nevada.

2. In his complaint, Mr. Munoz alleges that his local telephone lines are not secure and this alleged lack of security has caused his adult oriented business to lose money. Specifically, Mr. Munoz claims that unknown third parties have diverted incoming telephone calls away from his business to competitors or blocked them altogether.

3. Mr. Munoz admits in his complaint that these same issues were tried before the Nevada Public Utilities Commission (the "Commission"), in Docket No. 00-6057, and his Complaint makes numerous references to that administrative proceeding.

4. In that Commission proceeding, Mr. Munoz was represented by counsel of his own choosing and received a full and extended evidentiary hearing on the merits of his allegations and claims.

5. On September 23, 2002, the Commission issued an order dismissing Mr. Munoz's Complaint. Complaint, Exhibit B; Motion to Dismiss; Exhibit A. In that Order, the Commission made a number of findings of fact, including the following:

a. The record did not present any evidence that Sprint had caused call diversion and/or call blocking to occur (¶ 14);

b. Mr. Munoz's expert witness, Kevin Mitnick, was never able to recreate a situation where a telephone call was diverted to a competitor (¶ 14);

---

[1] Pursuant to Fed. R. Civ. P. 12(b)(6), this Court accepts as true the well pleaded allegations of the Complaint for the purposes of this Motion to Dismiss only.

c. Mr. Munoz's witness Kevin Mitnick testified that he did not know if Mr. Munoz's calls were being blocked or diverted (¶ 14);

d. Evidence was offered or other possible causes for Mr. Munoz's claimed problems, none of which were attributable to Sprint (¶ 14);

e. Mr. Munoz failed to present substantial evidence that call blocking and/or call diversion was being caused by Sprint (¶ 15);

f. Mr. Munoz failed to present sufficient evidence that Sprint "had failed to take the necessary precautions to insure the security of its network" (¶ 16); and

g. Sprint has "taken reasonable steps to protect its network" and its network security "is no better or worse than that of other telephone companies" (¶ 18).

6. Mr. Munoz concedes that he never sought judicial review of the Commission Order, and thus never appealed the Commission's findings and conclusions, despite the fact that N.R.S. § 233B.130(2)(c) requires a party to seek judicial review "within 30 days after service of the final decision of the agency."

II.
LEGAL ARGUMENT

A. Standard of Review on Motion to Dismiss.

Pursuant to the Federal Rules of Civil Procedure, a defending party may move for the dismissal of a complaint on the grounds that the pleading fails to state a claim upon which relief may be granted. Fed. R. Civ. P. 12(b)(6). Such a motion may be directed at all or less than all of the claims raised. Hon. William W. Schwarzer, et al., ***Federal Civil Procedure Before Trial*** § 9:189 (2000). A Rule 12(b)(6) motion must be granted if "it appears to a certainty that {Plaintiffs} would be entitled to no relief under any state of facts which could be proved." ***NL Indus.,Inc. v. Kaplan***, 792 F.2d 896, 898 (9th

Cir. 1986). For the purposes of a Rule 12(b)(6) motion, that claimant's allegations are generally assumed to be true and viewed in the light most favorable to the claimant. ***Id.*** However, the court need not accept as true conclusory allegations of law made in the complaint, nor must it accept unreasonable inferences or unwarranted deductions of fact. Schwarzer at § 9:221 (2000), ***citing In re Delorean Motor Co.,*** 991 F.2d 1236, 1240 (6th Cir. 1993). Material property submitted with a complaint, such as a attached exhibit, may be considered as part of the complaint for the purposes of a Rule 12(b)(6) motion. ***Hal Roach Studios v. Richard Feiner & Co.,*** 896 F.2d 1542, 1555 (9th Cir. 1990).

B. Mr. Munoz's Claims Are Barred by the Doctrine Res Judicata.

"The doctrine of *res judicata* provides that a final judgment on the merits bars further claims by parties or their privies based on the same cause of action." Headwaters inc. v. U.S. Forest Serv., 382 F. 3d 1025, 1028 (9th Cir. 2004) (citation and quotation marks omitted). Federal courts give a state judgment the same preclusive effect it would have in state court. ***Coeur D'Alene Tribe of Idaho v. Hammond***, 384 F.3d 674, 688 (9th Cir. 2004). Under Nevada law, the elements of res judicata are (1) an identity of claims in both actions, (2) a final judgment on the merits, and (3) the party against whom res judicata is asserted must have been party to the prior action, or in privity with a party to the prior action. ***Executive Management, Ltd. V. Ticor Title Ins. Co.,*** 114 Nev. 823, 835-36,963 P.2d 465, 473 (1998); ***see also Ayala v. Caesars Palace***, 119 Nev. 29, ___n.6, 71 P.3d 490, 492 n.6 (2003). If a plaintiff brings suit and fails to recover, he is barred from recovering on "all grounds of recovery that were asserted in [the prior] suit, ***as well as those that could have been asserted." University of Nevada v. Tarkanian***, 110 Nev. 581, 600, 879 P.2d 1180, 1192 (1994) (emphasis added).

Mr. Munoz makes the same allegations that he raised before The Commission – that Sprint damaged his business his business operations by failing to

provide an adequately secure telephone network. His first two claims for relief unabashedly request that this Court overturn the Commission Order. In fact, the Complaint repeatedly quotes from Regulatory Operations Staff's brief to the Commission[2], seeking to re-litigate the facts tried before the Commission in federal court.

An administrative agency's quasi-judicial decision is entitled to preclusive effect once it has become final an is o longer open to appeal. ***Int'l B'hood of Elec. Workers, Local 532 v. Brink Const. Co.*** 825 F.2d 207, 213 n.10 (9th Cir. 1987). Under N.R.S. § 233B.130(2), the time for Mr. Munoz to file a petition for judicial review of the final Commission Order dismissing his complaint was thirty (30) days, which has now long passed. Mr. Munoz was a party to the Commission proceedings, was represented by counsel, and received a full evidentiary hearing on the merits of his claims. Accordingly, Mr. Munoz's claims must be dismissed with prejudice on res judicata grounds.

C. 47 U.S.C. § 258 Does Not Create a Private Right of Action on Behalf of a Subscriber.

Mr. Munoz's third claim for relief is alleged under 47 U.S.C. §258 (a). This statute deals with illegal changes to "a subscriber's selection of a provider of telephone exchange service," and has nothing to do with the factual allegations set forth in the Complaint. Regardless, this claim must be dismissed because Section 258 is an inter-carrier statute, and thus creates a private right of action on behalf of "the carrier previously selected by the subscriber" only. 47 U.S.C. § 258(b). Section 258 (a) does not create a private right of action by a telephone subscriber against its carrier.

---

[2] Although the Complaint refers to this Staff's brief as an order by the Commission, it is not. Regulatory Operations Staff participates in contested cases before the Commission as "an independent party" and does not have the power to issue orders. N.R.S. § 703.301 (1). As a result, the legal briefs of Regulatory Operations Staff have no legal force or effect. They are simply legal briefs of a party to the proceeding. Significantly, though, Mr. Munoz does not dispute that even that Regulatory Operations Staff recommended that Mr. Munoz's administrative complaint be dismissed.

In support of his opposition, Mr. Munoz relies on several decisions defining the jurisdiction of state regulatory commissions under the Telecommunications Act of 1996 to arbitrate and enforce interconnection agreements between incumbent local exchange carriers (the established telephone companies in 1996) and competitive local exchange carriers (the new telephone carriers competing with established companies) under 47 U.S.C. §252. ***See Pacific Bell v. Pac West Telecomm, Inc.*** 325 F.3d 1114(9th Cir. 2003); **U.S. West *Communications, Inc. v. Sprint Communications Co., L.P.***, 275 F.3d 1241, (10th Cir. 2002); ***Southwestern Bell Tel. Co. v. Connect Communications Corp***., 225 F.3d 942 (8th Cir. 2000); ***Iowa Utilities Bd. v. F.C.C.,*** 120 F3d 753 (8th Cir. 1997), aff'd in part, rev'd in part sub. nom. AT & T Corp. v. Iowa Utilities Bd., 525 U.S. 366 (1999). This argument is without merit. Mr., Munoz is not a local exchange carrier. Because Mr. Munoz's claims involves a consumer complaint against a public utility, and not an interconnection agreement among public utilities, these cases are inapplicable to this case. Therefore, this claim must fail.

D. Munoz's Fourth Claim for Relief Does Not Allege that Sprint Acted Under Color of State Law.

Mr. Munoz's fourth claim for relief must additionally be dismissed because he does not allege that Sprint acted under color of state law. '42 U.S.C. § 1983 creates a private right of action against individuals who, acting under color of state law, violate federal constitutional or statutory rights." ***Squaw Valley Development Co. v. Goldberg***, 375 F.3d 936, 943 (9th Cir. 2004) (citation and quotation marks omitted). Sprint is private business entity, and even though its business is subject to 'extensive regulation" by the state, it does not act under color of state law. Scott v. Eversole Mortuary, 522 F.2d 1110, 1115 (9th Cir. 1975). Therefore, this cause of action fails as a matter of law and is without merit.

III.

CONCLUSION

Count I and Count II of Mr. Munoz's complaint are barred by the doctrine of res judicata. Count III must be dismissed because Mr. Munoz does not possess a private right of action under 47 U.S.C. §258. Count IV, which asserts that Sprint violated Mr. Munoz's constitutional rights under 42 U.S.C. §1983, fails as a matter of law because there is no allegation that Sprint acted under the color of state law. Accordingly, this Court hereby dismisses the above-entitled action with prejudice. Because the forgoing issues fully adjudicate Mr. Munoz's claims, this Court need not consider Sprint's remaining arguments in support of dismissal.

IT IS SO ORDERED.

(s) _____

UNITED STATES DISTRICT JUDGE

DATED: FEBRUARY 8, 2005

Submitted by

(s) _____

Patrick J. Reilly, Esq.
Thomas R. Ryan, Esq.
Hale Lane Peek Dennison and Howard
2300 West Sahara Avenue, 8th Floor, Box 8
Las Vegas, Nevada 89102

Attorneys for Defendant

APPENDIX F

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

EDDIE PAUL MUNOZ, Plaintiff- Appellant, v. CENTRAL TELEPHONE COMPANY- NEVADA; et al., Defendants - Appellees.	No. 05-15295 D.C. No. CV-04-01212-RCJ District of Nevada, Las Vegas ORDER

Appellees' motion to strike, any response to the motion and any related filings shall be referred to the merits panel for resolution.

For the Court:
Cathy A. Catterson, Clerk
(s)
Cole Benson, Deputy Clerk
9th Cir. R. 27-7/Note to Rule 27-7/
Rule 27-10

pro 8.1.05

APPENDIX G

NOT FOR PUBLICATION
UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

EDDIE PAUL MUNOZ,
Plaintiff – Appellant,
v.
CENTRAL TELEPHONE COMPANY NEVADA; et al.,
Defendants – Appellees.

No. 05-15295
D.C. No. CV-04-01212-RCJ
MEMORANDUM*

Appeal from the United States District Court
For the District of Nevada
Robert C. Jones, District Judge, Presiding
Submitted March 8, 2006**

Before: CANBY, BEEZER, and KOZINSKI, Circuit Judges.

Eddie Paul Munoz appeals pro se from the district court's judgment dismissing his 42 U.S.C. § 1983 action alleging Central telephone Company – Nevada ("Sprint") failed to maintain a secure telephone network, resulting in the loss of some calls to his business. We have jurisdiction under 28 U.S.C. § 1291. We review de nova a district court's judgment based upon res judicata. See Headwater Inc. v. United States Forest Serv., 399 F. 3d 1047, 1051 (9th Cir.2005). We affirm.

The district court properly concluded this action is barred by res judicata because Munoz raised, or could have raisd, these claims in prior administrative proceedings against Sprint before the Public Utilities Commission of Nevada. See Owns v. Kaiser Found. Health Plan, inc., 244 F. 3d 708, 713 (9th Cir. 2001); Britton v. City of North Las Vegas, 799 P. 2d 568, 569

(Nev.1990) (per curiam) (res judicata applies to administrative proceedings in Nevada); see also UOP v. United States, 99 F. 3d 344, 347 (9th Cir. 1996) (d0ctrine of administrative finality bars challenges to administrative descisions after the time for making a challenge has expired).

Munoz's remaining contentions lack merit.

AFFIRMED.

APPENDIX H

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

EDDIE PAUL MUNOZ,
PLAINTIFF – Appellant,
v.
CENTRAL TELEPHONE COMPANY – NEVADA; et al.,
Defendants – Appellees.

No. 05-15295
D.C. No. CV-04-01212-RCJ

JUDGMENT

Appeal from the United States District Court for the District of Nevada (Las Vegas).

This cause came on to be heard on the Transcript of the Record from the United States District Court for the District of Nevada (Las Vegas) and was duly submitted.

On consideration whereof, it is now here ordered and adjudged by this Court, that the judgment of the said District Court in this cause be, and hereby is **AFFIRMED.**

Filed and entered 03/29/06

APPENDIX I

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

EDDIE PAUL MUNOZ,
Plaintiff – Appellant,
v.
CENTRAL TELEPHONE COMPANY – NEVADA; et al.,
Defendants – Appellees.
No. 05-15295

DC# cv-04-01212-RCJ
District of Nevada
(Las Vegas)

ORDER

§Judges

The panel has voted to deny the petition for panel rehearing.

The full court has been advised of the petition for rehearing banc ad no judge has requested a vote on whether to rehear the matter en banc. See Fed. R. App. P. 35.

The petition for panel rehearing and the petition for rehearing en banc are denied.

No further filings will be accepted in this closed case.

2

Oct. 30, 2006

No. 06-1222

In the
Supreme Court of the United States

EDDIE PAUL MUNOZ; PRO SE,
- Petitioner

v.

CENTRAL TELEPHONE COMPANY NEVADA; ET AL
-Respondents

On Petition for a Writ of Certiorari to the United States Court of Appeals for the 9th Circuit

APPENDIX J-M
VOLUME 1

EDDIE PAUL MUNOZ ; Pro Se
P.O. BOX 61344
LAS VEGAS, NEVADA 89160
702-207-6411

APPENDIX J

PGS 42-68

MEMORANDUM OF LAW IN

SUPPORT OF INFORMAL BRIEF

Docket No. 00-6057
RH-7

PUBLIC SERVICE COMMISSION OF NEVADA
MEMORANDUM

DATE: NOVEMBER 22, 1996
TO: The Commission
Via Terry Page, DRO
FROM: Rick Hackman, Consumer Division
SUBJECT: Agenda No. 32-96, Item No.__.
Docket No. 96-11037, CCU-080295-AD, TKO vs. Sprint/Central Telephone Co.

I. SUMMARY OF COMPLAINT

TKO runs a Las Vegas escort/entertainment service. The company contends that in recent years, the number of incoming calls has dropped off considerably and in some cases, calls may have been diverted to a competitor. Centel has investigated its network and found no evidence of illegal tie-ins. Staff recommends the complaint be dismissed.

II. ANALYSIS AND INVESTIGATION

The complaint was filed in July 1995. TKO contends that in the last two to three years its business has dropped off by 50 percent. It further contends that on numerous occasions it has received a customer call and dispatched an entertainer to a given address only to discover that another entertainer from a competing agency is already there. TKO believes that the competitor has somehow obtained access into TKO's incoming lines and in some cases has prevented calls from going through.

In a written response to the complaint, Centel advised Staff that its security department investigated TKO's telephone lines and found no illegal connections or other devices on the lines. The utility also made several test calls to TKO from different locations in Las Vegas and the calls rang through normally. TKO was informed

that Centel's investigation had turned up negative results. On September 1, 1995, the Consumer Division advised TKO that Centel had followed established rules and regulations and had turned up no evidence of an illegal intrusion into its network.

Staff received several subsequent letters from TKO questioning our findings, however, the complainant did not ask that the matter be appealed to the Commission. We were recently advised by Centel that TKO had filed suit against Centel alleging the telephone company is somehow involved in collusion with the alleged call diversion. Centel has requested that the Commission review the matter so that the administrative process can be completed and the case can proceed in court.

III. DISCUSSION

The complaint received from TKO is one of four complaints received since 1995 from entertainment services. In each case, Centel has inspected both its facilities and facilities at the customers' locations and discovered no taps or tie-ins. In each case, the utility has called the customers' business from various locations and the calls have been received. In two cases, Centel installed monitoring equipment to mechanically count the number of incoming calls. The customer was asked to manually count the calls received. In both cases, Centel counted far more calls placed than the consumer reported receiving. Centel speculated that some customers were hanging up just as the connection was made.

Despite Centel's findings, it does appear to Staff that something is amiss since four separate entertainment services have reported the same problem. TKO has suggested that some hotels and motels have programmed their switchboards so that calls placed to these entertainment services are not put through. The entertainment industry has even gone so far as to place advertisements in adult-oriented publications urging potential customers to place calls from payphones so as to circumvent hotel switchboards. (Attached).

Staff believes this may be a partial explanation, although we have no firm evidence that it is the sole reason for the reported drop off of incoming calls. Centel has advised us that extensive testing has found nothing to indicate that its network has been penetrated. Staff does not have the resources or the expertise to independently check the integrity of Centel's network. If it is correct that hotels are somehow tampering with these calls, the diversion is taking place in non-utility facilities before the calls are passed through the utility network. Neither Staff nor Centel has the authority to investigate these areas.

IV. NOTICE AND SUBSEQUENT ACTION

Both parties in this case have been advised that the matter will be placed on the Commission's December 2, 1996 Agenda.

V. CONCLUSION AND RECOMMENDATIONS

Staff has seen no evidence that Centel is involved in a plot to divert telephone calls to entertainment businesses. To the contrary, the utility has investigated its facilities and found no evidence they have been breached. If blocking or diversion is taking place, it may be taking place outside the utility network.

Staff recommends that the Commission determine that no probable cause exists and dismiss this complaint so that civil litigation can go forward.

PUBLIC SERVICE COMMISSION OF NEVADA
MEMORANDUM

DATE: MAY 31, 1996
TO: Barry Holt
FROM: Rick Hackman
SUBJECT: Pellegrini vs. Centel, CCU-040496-AD

Barry, this must be the third or fourth escort service to allege that calls are being diverted.

Nevertheless, Centel says they find nothing every time they investigate. There has got to be something going on here. Please give me a list of these complaints so that we can pursue this a little further. Do you believe this is a mere coincidence?

RH: jkf

From: HACKMAN (Rick Hackman)
To: HOLT
Subject: Show World vs. Centel
Message-id: 32181B3101DEDEDE

Barry, I have reviewed the letter from the complainant's attorney and I recommend the following course of action: Have Centel provide you with whatever test results they have as well as some sort of a narrative summarizing what tests were conducted and what they purport to show. I'd like to know whether Centel tested the line electronically or whether they did any sort of a physical inspection for tie-ins. We'll decide later whether to turn it over to the attorney, although I can't see any reason why we should not do so.

I'm bothered by the fact that there is such a disparity between the calls counted by Centel and the calls counted by the complainant. If we accept Centel's explanation for the disparity, we have to assume that almost 60 people hung up before the call rang through. If you or I were calling an escort service, we naturally would chicken out at the last minute, but I don't know that the rest of their potential customers are as cowardly as we are.

I'm also troubled by the fact that you have had one or more similar complaints from other escort services. That indicates that something weird is going on.

Nevada Bell tells me that they agree there is no equipment they could or would install at the customer's premises to count incoming calls.

It seems to me that if calls are being diverted, they would have to be diverted to a location very near the complainant's premises because in order to divert calls, you have to run a wire from Point A to Point B. Perhaps this is possible if there are a couple of escort services in the same building, or block.
I think the bottom line is that we need to be able to assure ourselves that Centel has in fact taken all reasonable steps to assure themselves that there are no tap-ins on their side of the protector. To do that, we need to learn more about what they have done. We then need to tell the customer that he needs to hire someone to inspect his facilities to insure that no one has tapped in on that end.

PUBLIC UTILITIES COMMISSION OF NEVADA
Docket No. 00-6057
PREPARED DIRECT TESTIMONY OF RICK HACKMAN

1. Q. **Please state your name and the position you hold.**
A. My name is Rick Hackman; I am the manager of the Consumer Complaint Resolution Division of the Public Utilities Commission of Nevada's Regulatory Operations Staff ("Staff").
2. Q. **Does Attachment RH-1 contain your background and qualifications?**
A. Yes.
3. Q. **What is the purpose of your testimony?**
A. I will provide the Commission with a summary of the background surrounding Mr. Eddie Munoz's complaint, as well as other similar complaints received by the Consumer Division since the mid 1990's. I will also describe the test calls that I made earlier this year in the course of investigating this complaint. Finally, I will give my opinion on the quality of the investigations that Sprint conducted on several of these complaints.

4. Q. **Mr. Hackman, when did Mr. Munoz first file a complaint with the Division?**

A. According to our files, Mr. Munoz's first complaint was received on February 24, 1994. I have attached it and marked it as Attachment RH-2.

5. Q. **What was the nature of Mr. Munoz's complaint?**

A. Mr. Munoz's complaint has numerous allegations. He alleged that there was eavesdropping occurring on his business lines, his telephone service was being turned on and off, his bills had been altered, his calls were being intercepted, and other miscellaneous complaints relative to the complaints relative to the quality of the telephone service.

6. Q. **What did the Consumer Division do in response to this complaint?**

A. We created a formal complaint file and directed Sprint to provide Staff a written response. After receiving Sprint's response, we wrote to Mr. Munoz on April 6, 1994 with our findings. That letter is attached and has been marked Attachment RH-3.

7. Q. **What did you advise Mr. Munoz in that letter?**

A. That letter covers several points including: a. since some of his business lines had been cancelled several years before he filed his written complaint, repair and trouble records no longer existed; b. personnel recalled looking into his complaints the previous year, but could find no trouble; c. while Sprint was responsible for insuring that this network was secure, they were not a law enforcement agency; d. because Mr. Munoz's complaint suggested that criminal activity was taking place, we advised him to seek legal counsel. We believed that law enforcement was the appropriate entity to investigate complaints of eavesdropping and similar criminal behavior.

8. Q. **Did Mr. Munoz ask to have the Consumer Division's findings reviewed by the Commission?**

A. No, he did not.

9. Q. **What was the next complaint of this nature received by the Consumer Division?**

A. The next complaint was a year later in July 1995. The complaint was submitted by Ms. Hilda Brauer, owner of T.K.O. Inc. T.K.O. also provided entertainers in response to telephone requests. Ms. Brauer complained that she had seen a serious drop off in business in recent years which she attributed to telephone tampering. She reported sending entertainers to hotel rooms only to find that an entertainer from a competing business had already been dispatched to the room. She also claimed that she could hear clicks on her line and that calls frequently dropped off. She noted that she was receiving fewer and fewer calls from hotel rooms. I have attached her letter and marked it Attachment RH-4.

10. Q. **What did the Consumer Division do with Ms. Brauer's complaint?**

A. We again set it up as a formal complaint and directed Sprint to provide us with a written response. We then wrote to Ms. Brauer on September 1, 1995 with our findings. That letter is attached as Attachment RH-5.

11. Q. **What did that letter say?**

A. As with the Munoz complaint, we advised Ms. Brauer that Sprint had inspected its network for illegal connections or other devices and that none had been found. We also advised her that Sprint's test calls went through normally, we again advised the complainant that Sprint is not a policing agent.

12. Q. **Did Ms. Brauer appeal Staff's findings to the Commission?**

A. No, she did not. Ms. Brauer and her husband William sent several follow up letters, but they never asked that the issue be reviewed by the Commission. In their follow up letter, the Brauers contended that they and other owners of adult-oriented businesses believed that various hotels were preventing their guests from calling these adult businesses by blocking certain numbers at the hotel switchboard. The Brauers provided Staff with an ad from an adult publication which explained this theory. It is attached as Attachment RH-6.

13. Q. **What happened to the T.K.O. complaint?**

A. About a year after we wrote back to T.K.O., Sprint advised us that T.K.O. had filed suit against them in District Court. Sprint requested that the merits of T.K.O.'s complaint be ruled upon by the Commission so that the administrative process could be completed and the matter could proceed to District Court.

14. Q. **Did the Commission review the T.K.O. complaint?**

A. Yes, on November 22, 1996, Staff provided the Commission with a briefing memo summarizing the T.K.O. complaint. That has been attached and marked Attachment RH-7. In that memo, we also advised the Commission that at that time we had received four complaints from owners of adult entertainment services, all alleging basically the same thing. We informed the Commission that in each case, Sprint had investigated its network and found no evidence of a security breach. We pointed out, however, that it was possible that blocking or diversion could be occurring outside Sprint's network.

15. Q. **What was the outcome of the Commission's review of the T.K.O. complaint?**

A. After the complaint was presented to the commission by Staff, Ms. Brauer was asked if she wanted to address the Commission. My recollection is that Ms. Brauer said nothing. The Commission then voted 5-0 to dismiss the complaint.

16. Q. **Aside from complaints from Mr. Munoz and T.K.O., did Staff receive other similar complaints?**

A. Yes, in 1995 and 1996, we processed several written complaints from other adult-oriented businesses. They all suggested that diversion or other mischief was taking place, causing them to lose business.

17. Q. **Did Staff notice a pattern in these complaints?**

A. We did. It did strike us as odd that multiple businesses in the same industry were describing a similar problem. It seemed more than a coincidence.

Our difficulty was however that Staff had no means to independently investigate the Sprint network. Staff's telecommunications resources in the mid-90's were quite limited and consisted primarily of financial analysts

and economists. We had no telecommunications engineers, switch engineers, or other specialists intimately familiar with telephone hardware. As, such we could not conduct a physical inspection of Sprint's system to look for evidence of call diversion.

Instead, we relied upon Sprint's own internal investigations. In each case, we were assured by Sprint that they had investigated their network and found no evidence of call diversion. They also advised us that Sprint's investigators had placed test calls and those calls went through. Sprint further advised us that in some cases, they had attached counting equipment to the incoming lines of some adult businesses. Some of these counts showed many more incoming calls than the business owners reported answering.

Another problem that Staff encountered was that the local Sprint network represented only a portion of the calling chain. A call placed from a hotel room had to first move through the hotel's telecommunications facilities, including the hotel switchboard, or PBX. T.K.O. and others in the entertainment industry had already advised Staff that they believed some hotels were blocking their guests from completing calls to the complainants' businesses. This would certainly help to explain why these businesses were seeing a drop off in calls. Many of the entertainment businesses advertise in the yellow pages or in publications available up and down the Las Vegas Strip. Since hotel switch boards are programmable, it would seemingly be a simple matter for a hotel employee to note the numbers in these advertisements and program the PBX to not complete the call.

Hotel facilities, including the PBX, are owned and maintained by the hotel itself. Sprint cannot run tests on or otherwise investigate these facilities since they are outside the utility network.

Additionally, it is conceivable that if diversion was taking place, it could be occurring at the receiving end of the call. Sprint's facilities typically end on the exterior of a customer's premises where they connect with the customer-owned facilities. This commonly known as

the demark point. Presumably, blocking or diversion could be occurring somewhere between the demark point and the customer's telephone. Again, this is outside the Sprint network.

So, a call placed from a hotel room goes from the hotel's private facilities, across the Sprint network, and is delivered to additional private facilities on the receiving end. Sprint and Staff only had access to the Sprint network. It was like looking for a pea under one walnut shell and not being able to look under the other two shells.

18. Q. **Did Mr. Munoz file another complaint against Sprint?**

A. Yes, our records indicate that Mr. Munoz called in 1997 complaining that hotels were blocking their guests from calling his business. We advised him that we had no jurisdiction over the hotels themselves.

In December 1998, he again wrote and asked that we investigate his complaint against Sprint. He was advised that since the Commission had dismissed a similar complaint from T.K.O., Staff believed the matter had already been adjudicated at the Commission level. We declined to process his complaint.

19. Q. **What happened next?**

A. Mr. Munoz, through his counsel, requested a writ of mandamus in District Court asking the court to require that the matter be further investigated. Staff agreed to investigate further in exchange for Mr. Munoz withdrawing his lawsuit. Staff ultimately recommended that the Commission set the matter for hearing, which was done on February 22,2001.

20. Q. **Has Staff conducted any additional investigation in 2001?**

A. Yes, we have. We have contracted with Mr. Ron Bardarson, a computer and security specialist who has also filed testimony in this docket. We have served Data Requests upon the parties and we have participated in depositions and on-site inspections. During one visit to Las Vegas, I also placed several test calls to Mr. Munoz's business.

Mr. Munoz had previously advised me that he acts as a broker between escorts/entertainers and customers of such services. Mr. Munoz prints and distributes publications which contain ads and telephone numbers for these entertainers. When a call is placed, it goes to Mr. Munoz' office where he or an employee take the caller's hotel and room number. Mr. Munoz then calls the entertainer and if the entertainer later meets the hotel guest, Mr. Munoz has advised me that he receives a commission.

On August 6, 2001, I stayed at Harrah's Center Strip during a business trip. I picked up some street publications which I believed were linked to Mr. Munoz.

The publications were entitled "Informer" which is one of Mr. Munoz' businesses. Beginning at 8:45 p.m. I placed several calls to the numbers contained in the ads, most of which contained toll-free 866 or 888 prefixes. Mr. Munoz uses toll-free numbers to track his incoming calls.

Most of the calls were answered by a woman whom I believed to be a relative or employee or Mr. Munoz and to whom I had spoken on several occasions when calling him on his business line during the daytime hours. On a few occasions, a voice I recognized as Mr. Munoz answered the phone. I would either pretend to be an interested customer, or terminate the call after it was answered since I was concerned that after a while, my voice might be recognized.

21. Q. **Did all your calls go through?**

A. Yes, they did. Between 8:45 p.m. and 12:35 a.m. I made nine calls that all went through. The next day I made two more before checking out. They too went through.

22. Q. **Have other Staff members conducted similar tests?**

A. Yes, on occasion at my request and related to this docket other Staff members while on PUC business have placed calls from Las Vegas hotel rooms and advised me they rang through.

23. Q. **What did these test calls lead you to conclude about whether class placed from hotel rooms are being delivered to Mr. Munoz's business?**

A. I can only report that Staff's test calls went through just fine. We told none of the parties when we were going to make test calls or from where. WE saw no evidence of blocking or diversion.

24. Q. **In the course of investigation this complaint further, after the Commission had set it for hearing, did you learn more about Sprint's investigation?**

A. I did. On October 23, 2001, I participated in a deposition given by Mr. Robert Poole, an employee of Sprint. Mr. Poole was employed in the Sprint Security Division in the mid-1990s and investigated many of the complaints brought by Mr. Munoz and others.

25. Q. **What did Mr. Poole say about the nature of his investigations?**

A. Mr. Poole conceded that he was looking for evidence of eavesdropping, not call diversion. He testified that when investigating a complaint of call diversion he looked for evidence of a "left in wire" which would indicate that at some point, an illegal tap in had been made on the Sprint network in order to listen in on conversations. When asked whether a "left in wire" could be used to divert telephone calls, he admitted that it could not be used for that purpose. It appears, therefore, that Mr. Poole was looking for evidence that he was not likely to find.

Mr. Poole was also asked during the deposition whether in the course of his investigations, he had ever placed calls to Mr. Munoz's business from hotel rooms. This is significant because Mr. Munoz and his counterparts contended that while calls placed from payphones, cellular phones and residential phones rang through normally; calls placed from hotel rooms were allegedly being blocked or diverted.

Mr. Poole conceded that he did not place any test calls from hotel rooms. I have attached the relevant pages of Mr. Poole's deposition and marked it as Attachment RH-8.

26. Q. **Did Mr. Poole provide any investigative reports or other documentation showing the results of his security investigations?**

A. No, he said during his deposition that no reports were compiled and no records apparently exist to this day.

27. Q. **What was your reaction to these revelations by Mr. Poole?**

A. I was disappointed. As I noted earlier in my testimony, Staff did not have the resources to inspect Sprint's network, therefore we relied heavily on the results of Sprint's internal investigations. It seems that our reliance may have been misplaced. Mr. Munoz's witness Mr. Kevin Mitnick stated in his pre-filed testimony that he was able to obtain access to the Sprint network via diai up modem in 1995. Although he did not state that he actually rerouted calls, he implies that he certainly had the capability to do so. Meanwhile, Mr. Poole was looking for evidence of eavesdropping, not diversion, and looking fro physical tap ins to the network, not electronic ones. Finally, Mr. Poole did not even place any test calls from hotel rooms. These revelations came as a disappointment.

Staff and the Commission need to have confidence that when Sprint tells us they have investigated a matter, they have done a thorough and complete investigation. The Consumer Complaint Resolution Division relies heavily on the information provided to us by utilities and it is imperative that information be accurate and forthright. Anything less than that can result in a loss of credibility, not just to the company, but also to the Public Utilities Commission of Nevada.

28. Q. **Does that complete your testimony?**

A. Yes, it does.

Docket No. 00-6057
Exhibit No. 1 (RH-1)
Witness: Richard J. Hackman

QUALIFICATIONS AND EXPERIENCE OF RICHARD J. HACKMAN

EDUCATION Kent State University

Kent, Ohio Graduated 1973
Degree: Bachelor of Science, Journalism

WORK EXPERIENCE

July 1987 to Present — Public Utilities Commission of Nevada
Manager, Consumer Complaint Resolution Division

The Commission's Consumer Division acts as a liaison between the Agency and customer of the utilities and other entities which the Commission regulates. The Division attempts to mediate and resolve complaints brought against these regulated entities by their customers.

The Consumer Division acts as a repository for all complaint activity and statistics which the Agency receives. The Division maintains professional and clerical staff in both Carson City and Las Vegas, all of whom are supervised by the Manager.

November 1984 to July 1987 — Nevada Public Service Commission
Consumer Services Representative, Consumer Division

The Commission's Consumer Service Representatives receive, investigate and attempt to resolve inquiries and disputes brought by customers of regulated utilities and motor carriers. The Consumer Reps have significant public contact and are well versed in the regulatory process as well as most Commission rules, regulations and tariffs.

July 1982 to November 1984 — Attorney General's Office of Consumer Advocate, Reno
Administrative Assistant

Responsible for generating and channeling consumer interest in utility issues. Included writing press releases, meeting with consumer groups and keeping media informed of office's activities. Also acted as front line for most individual consumer complaints which came into the office.

1978 to 1981 Nevada Department of Energy
Deputy Administrator, Conservation and Planning Division

Responsible for overall supervision of public awareness activities. Included writing press releases, public service announcements, speeches, agency newsletter, etc.

1978 Journalist & Sunday Magazine Editor
Nevada Appeal, Carson City

Responsible for all phases of Sunday Magazine including writing, editing, page layout and photography. Also doubled as news and feature reporter for the daily newspaper.

1973 to 1978 Journalist
Las Vegas Sun & Review Journal, Las Vegas

Covered a variety of beats including District Court, municipal government and labor.

MEMBERSHIPS

NARUC Subcommittee on Consumer Affairs

EDDIE MUNOZ v. CENTRAL TELEPHONE COMPANY-NEVADA
TESTIMONY OF ROBERT POOLE
Pages 23-26
October 23, 2001

...one of your conversations, then I might employ a left in wire?

A: That possibly might exist because – as I tried to explain before, we use a cable with multiple appearance points. And on occasion, the wire is still left in at the old location. We reuse those facilities for the new location, and sometimes there's an instrument left at that old location.

Q: Did I also understand you to say, however, that a left-in wire could not be used to divert a call?

A: That's correct.

Q: So when Mr. Munoz and Ms. Brauer and others were coming to you with complaints about call diversion, why were you looking for a left-in wire if that couldn't cause diversion?

A: Because somebody could pick up that receiver or be listening to the call or whatever.

Q: But it wouldn't divert the call –

A: No. sir.

Q: -- it would just allow them to eavesdrop on the call?

A: No. sir.

Q: You said that on at least one or more occasions that you placed test calls –

A: Yes.

Q: -- to Mr. Munoz's business from various locations. I think specifically you said from using cellular phones, residential phones, and a few businesses.

A: We physically went to the Mirage and made test calls.

Q: Did you make those calls from rooms at the Mirage or from lobby phones?

A: Lobby phones.

Q: Did you ever, in the course of any of your investigations into Mr. Munoz's complaints actually get into rooms, actually rent rooms –

A: No.

Q: – or get access to rooms and place calls from there?

A: No. sir. I never did.

Q: Did Mr. Munoz tell you that he thought the source of his problem – did he tell you that he thought his problem was that he couldn't receive calls from hotel rooms themselves?

A: Yes.

Q: but you didn't actually go into any hotel rooms–

A: No.

Q: --and make calls from there? Okay. In the course of your investigation, either into Mr. Munoz's complaint or Ms. Brauer's did you have occasion to count the number of the incoming calls into one or the other of these businesses?

A: Larry Hill did that portion.

Q: You didn't do that directly?

A: No, sir.

Q: Did he share with you the results of those counts, not necessarily the numbers themselves, but did he give you some feel as to what he determined from counting those calls?

A: From what I recall is that the calls were originating and terminating from where they were supposed to.

Q: As a result of all of the time that you spent with Mr. Munoz and all the various investigations that you did on his complaints as well as Ms. Brauer's complaints – I recognize that you told us today that you never found anything – did you have a theory as to what was happening? Did you think that they were simply wrong in their perceptions, or what did you think?

Once you convinced yourself that there had been no intrusion on the Sprint network, what did you think in your own mind may or may not have been going on?

A: Well, I wanted to technically make sure that there wasn't anything wrong with the lines. I mean, that was my main function, my main job. I never came up with a good conclusion.

Q: So as long as the Sprint network was clean, that really was your only concern, and beyond that you were not interested in what might have been going on?

A: That's correct.

Q: Did you ever have course or reason to go to the hotels themselves and talk to P.B.X. supervisors about anything that might be causing this problem from the originating end?

A: We couldn't go to the hotels. They weren't in our – you know, we were mostly functioning on our particular switches, central office switches. We were not targeting another customer.

Q: And recognizing that that's hotel property, you didn't ask for their voluntary cooperation to help you try and get to the source of this?

A: No.

Q: Okay.

MR. HACKMAN: Okay. That's all I have.

Peter Alpert, Esq.
Nevada State Bar No. 3488
2950 East Rochelle Avenue
Las Vegas, Nevada 89121
(702) 866-6155
Attorney for Eddie Munoz

BEFORE THE PUBLIC UTILITIES COMMISSION OF NEVADA

Docket No. 00-6057

EDDIE MUNOZ v. CENTRAL TELEPHONE COMPANY-NEVADA, d/b/a SPRINT OF NEVADA.
Complaint alleging incoming calls are being blocked or diverted from customer's business.

EDDIE MUNOZ' MOTION TO COMPEL WITNESSES

Eddie Munoz, the Complainant herein, by and through his undersigned attorney, and pursuant to NAC 703.700, moves the Presiding Officer for an Order compelling the attendance of the following witnesses at the hearing commencing Thursday, March 14, 2002, in this docket. This Motion is made and based upon the following Memorandum of Points and Authorities.

I. POINTS AND AUTHORITIES

Pursuant to NRS 703.340(1) "Either party is entitled to an order by the commission for the appearance of witnesses or the production of books, papers and documents containing material testimony." Pursuant to NAC 703.690(1)(g), the Presiding Officer may issue appropriate interim orders.

Munoz respectfully requests that the Presiding Officer issue an Interim Order compelling the appearance of the following witnesses on Thursday, March 14, 2002, and any subsequent hearing days in this docket, for purposes of public comment and/or sworn testimony, as the Commission determines.

1. Gayland Hammack, Las Vegas Metropolitan Police Department.
2. Ray Brotherson, Las Vegas Metropolitan Police Department.

Munoz' request is necessitated by the fact that the law enforcement officials named above have conducted an extensive investigation into telephone call diversion allegations in the Las Vegas area and have information which may be relevant to this docket. Munoz incorporates by reference his Motion for Protective Order filed on March 6, 2002, which sets forth more specific facts.

Munoz respectfully asserts that Sprint has recently contacted the above-named officials' superiors as to the necessity of their testimony. As a result of that contact, the law enforcement officals cannot attend the hearing without a subpoena or attendance order from the Commission.

Based on the foregoing, Munoz respectfully requests that the Presiding Officer issue an order requiring the attendance of witnesses as set forth herein.

REPECTFULLY SUBMITTED this 12th day of March, 2002.

(s)_____

PETER ALPERT, ESQ.
Nevada State Bar No. 3488
2950 East Rochelle Avenue
Las Vegas, Nevada 89121
(702) 866-6155
Attorney for Eddie Munoz

OFFICE OF THE DISTRICT ATTORNEY
CIVIL DIVISION
500 S. GRAND CENTRAL PKWY.
P.O. BOX 552215
LAS VEGAS, NV 89155-2215
(702) 455-4761
Fax (702) 382-5178

STEWART L. BELL
District Attorney

MICHAEL D. DAVIDSON
Assistant District Attorney

MARY-ANNE MILLER
County Counsel

FACSIMILE COVER SHEET

To: Louise Uttinger, Esq.
Date: March 14, 2002
Fax #: 486-2595
Pages: 3, including this cover sheet

From: Mitchell M. Cohen Deputy District Attorney
Subject: Eddie Munoz v. Central Telephone Company – Nevada, d/b/a Sprint of Nevada Docket No. 00-6057

COMMENTS:
Operator: Afeni Banks Tele# 702/455-4761
Fax# 702/382-5178

If you have any problem receiving this transmission in its entirety, please contact the operator at the phone number above as soon as possible.

THIS MESSAGE IS INTENDED ONLY FOR THE INDIVIDUAL OR ENTITY TO WHICH IT IS ADDRESS AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, CONFIDENTIAL, AND EXEMPTION FROM DISCLOSURE UNDER APPLICABLE LAW. If the reader of this message is not the intended recipient or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone and return the original message to us at the above address via the U.S. Postal Service. Thank You.

March 14, 2002

Via Facsimile at 702-486-2595
Commissioner Adriana Escobar Chanos
Public Utilities Commission of Nevada
101 Convention Center Drive, Suite 250
Las Vegas, Nevada 89109

Re: Eddie Munoz v. Central Telephone Company Nevada -- Sprint of Nevada
Docket No. 00-6057

Dear Commissioner Chanos,

It has come to my attention of the Las Vegas Metropolitan Police Department ("LVMPD") that one of the parties to this action, Eddie Munoz, has sought to compel the testimony of two LVMPD officers with regard

to their knowledge of an investigation into the diversion of telephone calls by Sprint.

LVMPD is not a party to this proceeding, nor has it been directed to respond to any of the moving papers filed on behalf of Mr. Munoz. Nonetheless. The LVMPD wishes to apprise the Commission of its objection to any effort to compel its officers to testify before the Commission with regard to a criminal investigation.

As a procedural matter, it should be noted that the attendance of a witness before the Commission can only be compelled by a sanction of contempt through s subpoena or order issued by the district court. NRS 703.360;703.370. An order or subpoena issued by the Commission does not by itself compel a witness to appear. Furthermore, LVMPD policy prohibits members of the department from voluntarily testifying in civil actions, or testifying without being under subpoena. LVMPD regulation 4/108.07

LVMPD would oppose any order, and move to quash any subpoenawhich directed representatives of the Department to testify regarding a confidential law enforcement investigation. First, much of the information contained in intelligence investigation files consistsof nothing more than rumore, tips, and hearsay, not admissible evidence. Second, disclosure of such investigations would prejudice law enforcemtn. Disclosure of an investigation may expose the identities of confidential informants and undercover officers. It may reval the existence of investigatory efforts to current or potential targets. It may violate the privacy of individuals involved in the investigation. It may impar or destroy confidential investigative tequniquues and procedures.

A confidentiality agreement would not remedy the problem. The agreements used in PUC hearing are intended to protect trade secrets and proprietary information, not the records of law enforcemt investigations. It is doubtful whether the records of a criminal investigation could be shared with private parties and still reatian their priviledged charater. Even if the information remained technically privilegded, the harm to

law enforcement would still exist. A confidentiality agreement would be particularly inappropriate in this case, where the very parties before the Commission would to some extent be the subjectsof the alleged investigation.

For the forgoing reasons, th LVMPD expresses its objection to the issuance of any order or subpoena to compel the testimony of its officers regarding an alleged investigation into diversion of telephone calls by Sprint.

Sincerely,
STEWART L. BELL
DISTRICT ATTORNEY

By: (s)_____
MITCHELL M. COHEN
Deputy District Attorney

MMC:ab
Cc: Peter Alpert, Esq. (via facsimile at 382-0147)
Louise Uttinger, Esq. (via facsimile at 486-2595)
Rick Hackman (via facsimile at 775-687-6120)
Patrick Reilly, Esq (via facsimile at 365-6940)
Richard Hinckley, Esq (via facsimile at 486-2595)
Kathryn Landreth, LVMPD (via facsimile at 229-3191)

Louise Uttinger, Esq.
Nevada State Bar No. 1971
PUBLIC UTILITIES COMMISSION OF NEVADA
1150 East William Street
Carson City, NV 89701-3109
775/687-6002

BEFORE THE PUBLIC UTILITIES COMMISSION OF NEVADA

Filed: 02 Aug 22 PM 12:12
Docket No. 00-6057
EDDIE MUNOZ v. CENTRAL TELEPHONE

COMPANY-NEVADA, d/b/a SPRINT OF NEVADA. Complaint alleging incoming calls are being blocked or diverted from customer's business.

REGULATORY OPERATIONS STAFF'S REPLY IN OPPOSITION TO SPRINT'S REQUEST TO TAKE JUDICIAL NOTICE

Regulatory Operations Staff ("Staff") of the Public Utilities Commission of Nevada ('Commission"),pursuant to NRS 233B.123(5) hereby submits its Reply in Opposition to Central Telephone Company-Nevada d/b/a Sprint of Nevada's ("Sprint") request to take judicial notice as requested in Sprint's Post-Hearing Brief filed August 16,2002. Staff's Reply also informs the Commission that Sprint's pleading violates the Nevada rules of Administrative Practice ("NAC") for Rules for Practice Before the Commission.

I.

Sprint Should Not Be Allowed to Supplement to Record with Stale Information

Counsel for Sprint calls Mr. Munoz' witness Kevin Mitnick an expert at lying while simultaneously trying to supplement the record[1] to add a *Forbes* article[2] concerning a Federal Communications Commission ("FCC") licensure proceeding involving Mr. Mitnick's ham radio license. While Counsel writes that the *Forbes* article was published "Since the completion of this Commission's hearing...",[3] Counsel fails to disclose to the Commission that the FCC matter is old information. Significantly, Counsel also did not disclose whether Counsel or Sprint was aware of the FCC licensure proceeding against Mr. Mitnick prior to the *Forbes* article.

---

[1] Sprint's Post-Hearing Brief at 9. See footnote 4. Sprint asks the Commission to take "judicial notice" of the article. (Citations to Sprint's Brief are to page number only since the document was not on lined pleading paper.)

[2] Sprint's Post-Hearing Brief, faxed page 18.

[3] Sprint's Post-Hearing Brief at page 9.

The FCC proceeding dated December 21, 2001, is "old" news, as evidenced by the techlawjournal article attached to Staff's Reply as Exhibit A. A copy of the referenced FCC's Hearing Designation Order is attached as Exhibit B. Since the FCC Order, numerous articles have been written regarding the FCC-Mitnick proceeding. See exhibit C, "How American Taxpayer Dollars Are Spent" and Exhibit D, National Association for Amateur Radio article. Also see Exhibit E, "US to yank Kevin Mitnick's radio license" and Exhibit F, Letter regarding Amateur Radio license renewal application of Kevin Mitnick, N6NHG. While a hearing has been held in the FCC matter, no decision had been rendered.

Staff seriously doubts that Sprint or its Counsel was unaware of the FCC matter when it had the opportunity to cross-examine Mr. Mitnick on June, 24,2002. Staff therefore objects to Sprint's attempt to "supplement" the record with stale information that Mr. Mitnick could have responded to or rebutted in cross or re-direct examination during the hearing.

II.

Sprint's Pleading Violates NAC 703.560(1)(f)

Sprint fully participated in establishing the page limit for Post-Hearing Briefs in this case. Sprint regularly participates in cases before the Commission and its Counsel are well aware of the Commissions Rules for Practice.[4] Nevertheless, Sprint's filed Post-Hearing Brief in this case violates NAC 703.560(1)(f).

As the portion of the Transcript of Proceedings attached as Exhibit G reflects, Sprint's outside Counsel suggested a 10 to 15 page limit for post-hearing briefs[5]. Sprint's General Counsel restated Mr. Reilly's suggested 15 page limit to the Presiding Officer[6]. The Presiding Officer directed that written briefs be "No more than 15

---

[4] Sprint's earlier pleadings in this case were double spaced. See Memorandum of Points and Authorities in Support of Sprint's Objection to and Motion to Strike Portions of Testimony of Eddie Munoz and Kevin Mitnick, filed by Sprint on December 24, 2001.

[5] Tr. at 939, II. 19-22.

[6] Tr. p. 940, II.23.

pages."[7] Both Sprint Counsel participated in the case and jointly filed Sprint's Brief.

NAC 703.560(1)(f), Form of Pleadings, requires that pleadings filed with the Commission be double spaced, except for footnotes or quotations which are indexed. Sprint's pleading contains extensive argument that is single spaced[8]. If Sprint's electronic document were properly formatted, Sprint's Brief would exceed the Presiding Officer's 15 page limit.

Staff anticipates that Counsel for Mr. Munoz would take exception to Sprint's Brief based on page limitations, if he were available to do so. However, Mr. Alpert informed the Parties during the hearing that he was leaving for Europe on or about August 15, 2002. Thus, in fairness to opposing counsel and parties, Staff informs the Commission of Sprint's violation so that the Commission may take any action that it deems necessary.

Staff therefore respectfully requests that the Commission issue an Order that:

1. Denies Sprint's requests for judicial notice of the Forbes article, and

2. For such other and further relief as the Commission deems appropriate.

RESPECTFULLY SUBMITTED this 22nd day of August, 2002.

PUBLIC UTILITIES COMMISSION OF NEVADA
REGULATORY OPERATIONS STAFF
By: (s)_____
Louise Uttinger, Assistant Staff Counsel

---

[7] Tr. at 940, ll. 24-25.

[8] Sprint's Post-Hearing Brief at pages 5 and pages 11-13.

APPENDIX K

PGS A-69-83

P.U.C. DOCKET 00-6057

BATES RECORD 010512-010533

KANSAS CITY NETWORK

INTRASTATE –INTERSTATE

DOCUMENTED SS7 INTRUSION
EVENT P.U.C. DEPOSITIONS

BATES RECORD 011400-011401
011408.....PGS A-69-83

APPENDIX 5
KANSAS CITY NETWORK
NOMIS TROUBLE TICKET
P.U.C. DOCKET 00-6057
BATES RECORD
010512-010533

Nomis Ticket Incidents

Nomis tickets are internal problems of Sprint network.

Incident of T-1 span circuit ID code Nomis ticket 208 network problem of switch and translations of NOC Kansas City, Sprint Nortel network after hour weekend functions this issue was with technical assistance group. These problems that occurred were all Sprint network problems. I worked and tested with technical assistance superiors when problems were occurring which was documented by audio recording of call assistance during trouble tickets that corresponds with CEN bates the problem was that data/voice traffic was being process into trunks of circuits of sprints network switches that fulled up our trunks that were provided by Sprint switch and translation which caused 24 trunks to be busy and the 25 would drop or busy. The switch was manupted to appear technically it was ready to receive a call on the screen but was manupted to not show trunks were full of conversation. We even changed facility and it still was in the switch when the propriety problem of Sprints network was compromised Sprint stop all testing with me which is essential to coming to a truthful answers and you must test with the operator who answer the phone to see what is going on Sprint stop all communication and closed tickets out and stopped all positive testing.

11-19-01 NOMIS Ticket Incidents

CEN 2108, 2109, 2110

CEN 8-3, start
CEN 95, 96, 97, 98, 99, 100, 101

CENTRAL TELEPHONE COMPANY-NEVADA d/b/a SPRINT OF NEVADA'S RESPONSE TO EDDIE MUNOZ'S DATA REQUEST NOS. 1-9 DOCKET NO 00-6057

DATA REQUEST MUNOZ-1:
Requester: Munoz
Please provide copies of the following-described trouble tickets or repair requests:

Ticket Number	Date
137540	10/30/00
158701	11/27/00 or 1/18/01
5182948	11/30/00
152098	12/22/00 or 12/23/00
C820418	1/25/01
WB01263768	1/26/01
165240	2/10/01 or 2/12/01
165674	2/12/01 or 2/14/01
29376	2/20/01
WB0274824	2/27/01
173353	3/11/01 or 3/12/01
174113	3/13/01
173358	3/16/01
333461	3/24/01 or 3/25/01
208856	4/3/01
336805	4/3/01 or 4/4/01

RESPONSE TO MUNOZ DATA REQUEST-1:

The number 29376 is not a valid ticket number. In addition, Ticket no. 173358 and Ticket No. 208856 are not associated with Mr. Munoz' Sprint account, and will not be produced.

Please see **Exhibit "A"** attached hereto for documents that are responsive to this Request.

Responsible Person: Scott Collins
Date Prepared: May 30, 2001

SUPPLEMENT RESPONSE TO MUNOZ DATA REQUEST-1:
Please see Exhibit "A" attached hereto for documents (Bates numbered CEN 2107 through CEN 2110) pertaining to NOMIS ticket No. 208856 that are responsive to this Request.

Responsible Person: Scott Collins
Date Prepared: July 2. 2001

EDDIE MUNOZ v.
CENTEL TELEPHONE COMPANY NEVADA
EXHIBIT 4
SCOTT COLLINS TESTIMONY
October 23, 2001
(Pages 54-61 of transcripts)

BY MR. ALPERT:

Q: Is the Kansas City location of Sprint a main hub or a main office, or is it the place where most of the Sprint management is located?

A: Our Corporate headquarters is located—

Q: That's what I'm trying to say. Thank You. So that's Sprint's corporate headquarters?

A: Correct.

Q: Thank You very much for that. Maybe you ought to be deposing me.

Is any part of the Las Vegas network—telephone network monitored from Kansas City?

A: Yes.

Q: Explain to me how that is done.

A: I believe we have a division called the Network Operations Center, which has the ability to monitor Sprint's various local Telephone division's network.

Q: And when you say it can monitor the network, what do you mean by that?

A: The Network Operations Center, or NOC, has the ability to determine if there are any major cable cuts, any type of what's referred to as alarms which go off anytime there's a major outage within our network.

So they basically have the ability to make sure that everything's running smoothly. And if a problem develops, then they're able to take appropriate action.

Q: That work is generated from Kansa City?

MR. REILLY: Objection. Vague.

THE WITNESS: I believe they work- or observe our network during non-business hours. During normal business hours, we monitor it here in Las Vegas.

BY MR. ALPERT:

Q: You're monitored by Kansas City in Las Vegas, or are you monitored in Las Vegas by Las Vegas?

A: We monitor Las Vegas in Las Vegas during normal business hours—and not necessarily normal business hours. There may be certain individuals that work throughout the night. But after the majority of the central office forces go home, it's my understanding that the NOC then takes over.

Q: So at that point, the monitoring is to be done through Kansas City? Or am I misunderstanding what you're saying?

A: Again, it's just my understanding from speaking to people, through this case, that NOC is responsible for monitoring Sprints Las Vegas network when there is no one in Las Vegas monitoring the network. For example, if they've gone home or a shift has ended.

Q: Do you know if the NOC has ever monitored Mr. Munoz's lines during the time this case has been open?

A: I believe they have.

Q: When monitoring takes place, is some type of a written documentation generated to show the results of the monitoring?

A: Not necessarily, no.

Q: Well, hypothetically, if NOC was monitoring a line and it found something to be askew, would some type of a report be generated?

MR. REILLY: Objection. Calls for speculation. If you know.

THE WITNESS: I don't know.

BY: MR. ALPERT:

Q: Do you know who is in charge of that network?

A: No, I don't

Q: Can you explain to me what a NOMIS, N-O-M-I-S, ticket is.

A: I've never worked in these types of service order and repair tickets, but during the course of my investigation, I've learned about them. And I believe a NOMIS ticket is created for a technical assistance group in response to a repair ticket initiated by a Sprint subscriber.

Q: Does it contain information that a technical assistance group needs to do its work, or what is the purpose of NOMIS ticket?

A: I believe the process is that, when a Sprint subscriber calls in a service problem for a special circuit line or a complex line, there's a trouble ticket that's generated that's dispatched to the field forces.

And I believe a NOMIS ticket is created from that initial ticket for the technical assistance group to monitor the serving central office – the serving central office of the subscriber to make sure everything's programmed properly and whatnot.

And then if everything is okay, then it's dispatched to the field for the filed tech to work.

Q: Are those tickets maintained by Sprint in the same manner that service orders are?

MR. REILLY: Objection. Calls for speculation. If you know.

THE WITNESS: I don't know.

BY MR. ALPERT:

Q: In one of our data requests, we asked for a NOMIS ticket, and we were told that it was no available.

Do you know how log they are retained?

A: I don't know.

Q: Do you know who is in charge of retaining those documents?

A: No, I don't.

Q: Do you know what department is in charge of retaining those documents?

A: I think so.

Q: Okay. Let me hear it.

A: I think it's the technical assistance group.

Q: Is that a group that has presence in Las Vegas?

A: I'm not sure. I believe they have a presence in Kansas City. (Exhibit 10 was marked for identification and is attached hereto.)

BY MR. ALPERT:

Q: Let me hand you what's been marked as Exhibit 10, Mr. Collins. It's an email dealing with the subject – or piece of equipment called Foneview, F-o-n-e-v-i-e-w.

Can you tell me what Foneview is.

A: I believe Foneview is a product – or a service offered by Sprint that will provide the customer with form of called detail record reports.

Q: Is this something that Mr. Munoz has asked for in the past?

A: Mr. Munoz wanted daily called detail record reports, and Sprint was unable to provide him with those. He was having – Mr. Munoz was having some difficulty getting these reports. So I tried to make some calls myself and see if I could find a product or service that was applicable to Mr. Munoz's service. And one of those services was called Foneview.

Q: And what does it do?

A: It's similar to Mr. Munoz's long distance bill that is marked as Exhibit 7 in that it's a daily report that shows the date and the time, the number originating the

call, the number that was called, the duration of the call and whatnot.

It gives a detail of the calls that were made, and it's produced on a daily basis, whereas, I believe, Mr. Munoz's bill is produced on a monthly basis.

Q: What is the cost associated with that product?

A: I don't know what the cost is for Foneview.

Q: Did you discuss obtaining that service for Mr., Munoz?

A: Yes, I did.

Q: What was the result of those discussions?

A: I believe that Foneview was not applicable to Mr. Munoz's service.

Q: Why?

A: I believe it had to do with the type of service that Mr. Munoz had. I'm not sure why it wasn't applicable. But I know that it wouldn't work for Mr. Munoz's service.

Q: Is it a service – I'm assuming it's a service for commercial customers, not for residential customers.

A: I don't think so.

Q: Or am I wrong in my assumption?

MR. REILLY: Calls for speculation. If you know.

THE WITNESS: I don't know.

(Exhibit 11 was marked for identification and is attached under separate cover.)

EXAMINATION (Continued)

BY MR. ALPERT:

Q: I'm going to hand you what has been marked as Exhibit 11, which is Centel 636. Apparently – take a look at that and tell me what that is.

MR. REILLY: I believe this document has been designated as confidential, and I'd ask that this portion of the transcript be designated as confidential as well.

MR. ALPERT: That's fine.

(Upon instruction of counsel, the portion of this transcript following the above discussion has been marked confidential and is included under separate cover.)

BY MR. ALPERT:

Q: Mr. Collins, I want to spend just a couple moments on some of the responses to the data requests.

The PUC initially made some dated requests to Sprint in this case, which you responded to on May 10th of 2001.

Now, Data Request 3 asks to provide copies of any internal reports or investigations undertaken…

(Pages 86-88 of transcripts)

…Exhibit 14, which is Centel 300. a fax cover sheet. It says it was sent by you.

Is that your handwriting down there?

A: Yes.

Q: You see where it say 18 pages went with that?

A: Yes.

Q: Do you know what went with that facsimile cover sheet because that's all I have?

A: I don't recall what I sent to him.

Q: Is there a way you can go back in your records and determine what you did send to him?

A: I don't know if I can find that fax that I sent to him. This doesn't ring a bell at all.

Q: Would you please make an attempt, when you go back to your office, to see if you have – however you maintain your files, to see if you have a copy of that fax and the documentation of 18 pages that went with it?

A: Sure.

Q: Thank You.

Let me hand you what has been marked as Exhibit 13. You were talking about the NOC system before.

Is that a report form the NOC system?

A: I don't know.

Q: Have you ever seen a report similar to that?

A: I believe this is NOMIS Ticket Number 208656.

Q: Did that come from Kansas City?
A: Yes.
Q: And look on page 2 of that document. About halfway down, it talks about static, cross-talk, et cetera.
A: Yes.
Q: Is that what is being reported by the monitoring from Kansas City?
A: It appears that the technician investigating the problem found these problems associated with the various channels on Mr. Munoz's T-1.
Q: But that determination came from monitoring in Kansas City, not from Las Vegas?
A: I don't know.
MR. REILLY: Calls for speculation.
MR.> ALPERT: There's one more that I have. Let's mark this one
(Exhibit 15 was marked for identification and is attached hereto.)
BY MR. ALPERT:
Q: This is Exhibit 15. Is that document in your handwriting?
A: No, that's not.
Q: It talks about Belcore standards. Are you familiar with that – Belecore standards?
A: vaguely.
Q: Can you tell what that is, as you understand it?
A: I believe Belcore was developed after the fallout—or the braking up of AT and T. And I believe they were a lab that set standards for the various companies that had been split up by AT and T so everyone could internet with each other because it's important that all networks work together.
And I believe that Belcore is the authority on setting the standards for telecommunication devices.
Q: Do you know who wrote that note?
A: No, I don't.
MR. ALPERT: Okay. Thank You.
That's all I have.
THE WITNESS: Thank You.
MR. ALPERT: We're done.

(the deposition concluded at 12:37 p.m.)

Network Operations Management Information System
Operations Report Date/Time: 6/26/01 11:17 AM CDT
Page: 1

Primary Network Entity Summary ----------
Ticket Number: 208656
CLLI: LSVGNVXMDS0
Name: LAS VEGAS (EAST-7)
Host CLLI: LSVGNVXMDS0
Host Name: LAS VEGAS (EAST-7)
Eqp Role: Host Eqp Type: DMS-100
Eqp Vendor: Nortel Soft Ver: NA0011
Rven: Set Lvl:
ESA Eqpd?: No Working Lines: 27529
Access Lines: 27529 NOP Region: Western
OP Region: WO OP Sub Reg: NV
OP Area: NV OP District: Las Vegas
MSA?: LAS VEG
AS

NPA:	NXX:
702	430
702	432
702	440
702	457
702	486
702	641
702	654

Clec Names:
MGC
EASY CELLULAR INC
TEL-LINK
Sprint Internal
Nevada Telephone
Sprint Internal – NV

Cellular 7
Compass Telecom Inc.
Electrical Lightwave
COMM SOUTH
Reconex
Preferred Carrier Sv
Frontier Telemanagem
MAX-TEL COMM INC
Procell Electronics
US Telecom
Onesource Telecom
Alt. Tele. Connectio
NEXTLINK
QTEL
SPRINT NTS

Associated Entity Summary

CLLI	Name	Role	Type	Equipment	Type
Vendor		Lines	ESA		

Network Operations Management Information System
Operations Report Date/Time: 6/26/01 11:17 AM CDT
Page: 2

Request for Technical Assistance Summary ----------

Status: Closed Priority: MAJOR RCA Reqd?: No
Ticket Open Date/Time: 3/30/01 6:50:03 PM CDT
Opened By: Donald E. Lawver
Ticket Open Date/Time: 4/6/01 9:30:33 AM CDT
Closed By: Donald E. Lawver

Addressed To: Donald E. Lawver Work Group: TA
Cbr: (913) 791-2
Acknowledged Date/Time: 3/30/01 6:56:49 PM CDT
Requested By: Eddie CBR: 312-4378
Category: TRUNKING Study Code: NOCW
RIDE Ticket:

Request Description: Not all calls are completing to his trunk

Action Taken:
**** NEW ENTRY: 3/30/01 7:05:14 PM, by Donald E. Lawver ****
Customers trunk is COMPCONS00 on DTC 24 12, DID numbers are 44D-3500-99. Eddie says he is able to receive from cell phones, pay phones, long dist., and local. The only ones that fail are from hotels (but not all the time). Eddie worked with Security and they made test calls from the Sahara and Travel lodge and they completed, but security had the traffic report pulled and there are hotel origination numbers that failed on the report, also on the report numbers that were called from the hotels showed the wrong origination number. The way they know they had a failure the console lights up and when they answer there is a click and the call is gone. I am going to have the night crew pull some oms and watch the span.
**** NEW ENTRY: 3/31/01 5:44:24 AM, by Kenneth J. Keltner ****
I MONITORED LOGS OFF AND ON ALL NIGHT SAW NOTHING UNUSUAL.
****NEW ENTRY: 3/31/01 4:52:11 PM, by Donald R. Lawver ****
Tested with Eddie performed a onoffhk on each channel when he answered call most was dead air except for channels listed below which have crosstalk and static.

Channels:
6= Static
7= Crosstalk
8= Crosstalk
10= Crosstalk
12= Crosstalk
15=Static
18= Static
20= Crosstalk
24= Crosstalk

****NEW ENTRY: 3/31/01 7:01:18 PM, by Donald E. Lawver****
A cable tech by the name of Al called in he is going to go out and move the span from DTC 24 12 to DTC 25 12. We have okay this with Eddie to take down for this short duration.
****NEW ENTRY: 4/1/01 5:28:44 PM, by Donald E. Lawver ****
The span did get changed last night but nobody did any testing with the Sprint Propriety Information – Unauthorized Disclosure Prohibited

Network Operations Management Information System Operations Report Date/Time: 6/26/01 11:17 AM CDT Page: 3

Customer to see if the noise was still on the channels or if crosstalk was present on any of the channels.
Nolan a cable tech put a t-com on the circuit all day and there was no errors. This is a HDSL circuit and the counters on this is clean. Customer is still having trouble.

****NEW ENTRY: 4/1/01 6:55:34 PM, by Donald E. Lawver****
I did the sgnl onoffbk with Eddie again we found crosstalk on 2-4, 7, 9-12, 14,15,17,20-22. I am guessing that all of the channels would show crosstalk if there was calls. The channels that I tested yesterday that had static on them I believe now was data I heard today the connection of the modem and then the data come across the same

****NEW ENTRY: 4/1/01 7:53:16 PM, by Donald E. Lawver****
Cable techs are going to talk about Monday morning and we can call 2-244-4088/4089 and see who has the ride ticket and what the counts on the bird look like Ride tckt number is 333.461
NEW ENTRY: 4/2/01 11:58:20 AM, by Ronald L. Kling*

Nolan called to say that the t-bird is clean for last night. The hdsl also looked clean along with the counters.
****NEW ENTRY: 4/6/01 9:29 AM, by Donald E. Lawver****
Per Kenny V this is going to be turned over to the Las Vegas guys Larry and Kai. Closing text.

Restart Summary

Role EQP Vendor SWVer SWRev SWPSL
Restart Type: Restart Class: Error Id:
Error Description:
Active CPU: Mem Loc: CPU Transfer?:
Duration: Restart Reason:
Action Taken:
RTA Coding Summary:
WO:

FO:
CA:
RS:

Sprint Propriety Information – Unauthorized Disclosure Prohibited

APPENDIX L

PGS A- 84-101

SPRINT NETWORK
P.U.C. DOCKET 00-6057

BATES RECORD 011206 -010355

P.U.C. SUPPORTING CASES OF
JURISDICTION HOTELS ABUSE

BATES RECORD 010355-010356

SPRINT MONOPOLY ARTICLE
REVIEW JOURNAL NEWSPAPER

APPENDIX 3
SPRINT NETWORK
DOCKET NO. 00-6057
BATES RECORD
011206-010355

(TEXT FROM A BOOKLET ENTITLED "Well Connected")

Sprint®
Central Telephone-Nevada

Well Connected
"Be There Now."

No one is as well connected as Sprint. Sprint has made the investment in both technology and people to keep you connected no matter what happens. That's important when you consider how much you have on the line. Imagine what it would cost you if something went wrong. Imagine customers not being able to reach you. Data and video transmissions unable to flow I and out of your company. Then ask yourself whether or not you can afford a discount communications provider.

The bottom line is no one keeps you more well connected in the valley than Sprint. But that should come as no surprise. After all, we've been in the valley since it all first began.

Back in those days, we were known as the Southern Nevada Telephone Company. **Then in 1961 we evolved into Centel. And in 1993, we took a step into the future, becoming Sprint/Central Telephone-Nevada.**

Through it all, one thing has remained the same. Our unparalleled commitment to keeping you connected no matter what. When you have Sprint on your side, you're well connected.

A world class inter-office network.

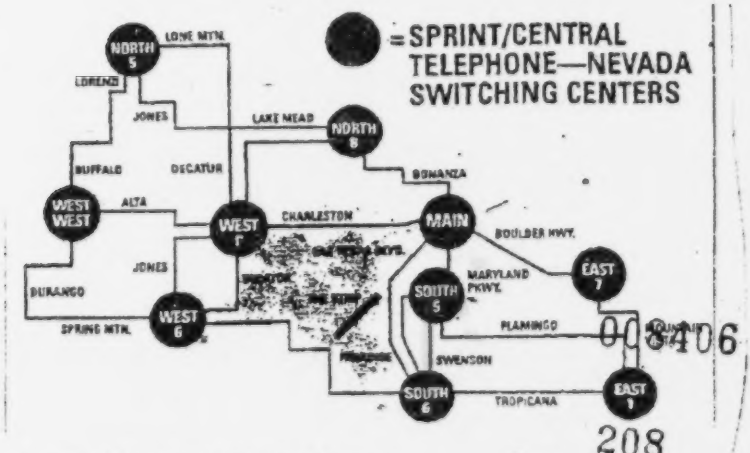
At any given time, you can reach any part of the valley with our inter-office **network of fiber optic trunking**. That's not just a promise. It's a fact.

With our system, we use a process we call **"self-healing."** If a line does go down because of a natural or man-made disaster, the system re-routes your call immediately. In fact, this system is so advanced, you'll never even know a problem occurred.

Unparalleled fiber optic distribution.

Your call travels through one of the greatest fiber optic route systems ever designed. To create this highly diverse system, we've strategically buried more than **450 miles of fiber optic cable** in conduit. This makes it much less susceptible to damage and deterioration than fiber strung on telephone poles. In fact, it represents some of the best protected cable ever created to resist the desert elements.

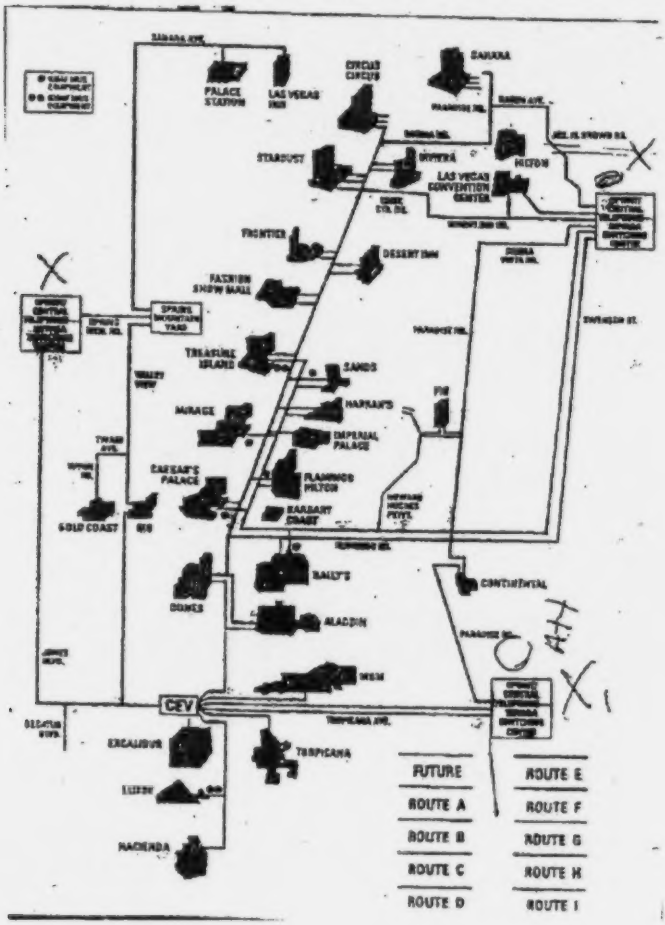
Once again, the system automatically re-routes your call if some disaster cuts a cable path. With Sprint's system, you know your call will always get through.



A map of the "core" Las Vegas network

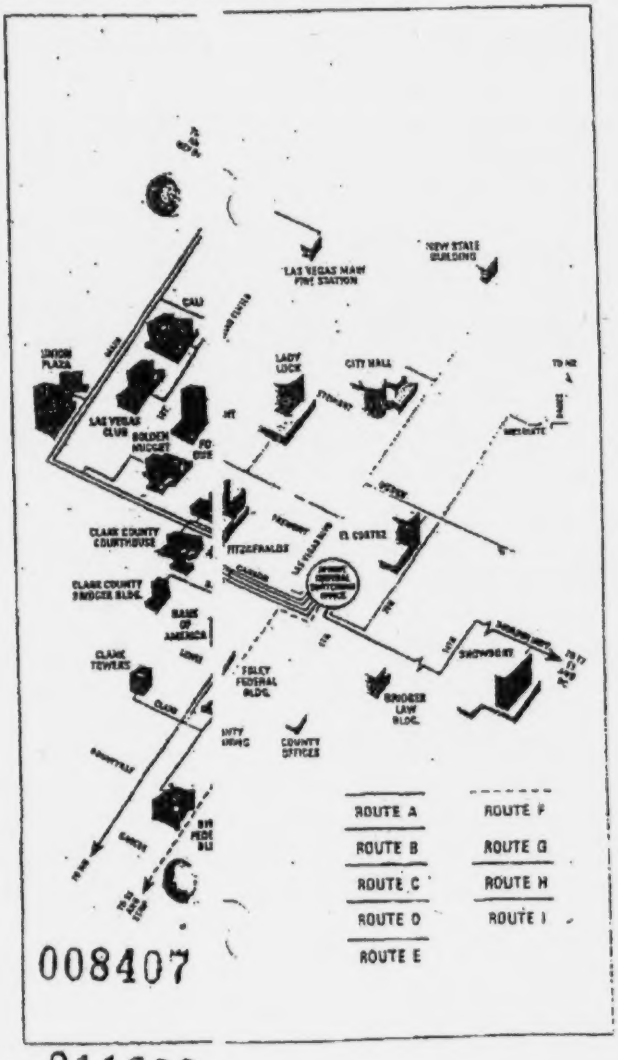
008406
208

Hotel/Casinos lining the "Strip" and the local fiber routes.



BEST AVAILABLE COPY

Hotel-Casinos downtown the local fiber routes.



008407

CEN 2074

Digital switching with back-ups on line.

Our **switching centers** are an integral part of the network. You can rest assured your calls and information flow uninterrupted through them for two reasons. First of all,

we have the very best technology in place to handle the large capacity. Second, we have identical **back-up equipment** on line. If a component fails, the back-up takes over. Again, you'll never even know there ever was a problem.

$2 million in local inventory.

If a disaster strikes, were ready with more than **$2 million worth of back-up** electronic inventory right here in Las Vegas. That means we can have you back in **service within minutes** rather than waiting with no telecommunications for parts to arrive in town. In fact, we did just that for the Luxor and the Excalibur. A flooded controlled environment vault destroyed the fiber distribution node. But with our people and inventory, we were able to have them back in service that same day.

$750 million investment. $55 million yearly upgrade.

We've made a $750 million investment to create an **all digital network** in the valley. And we've equipped it with a fully computerized, 24-hour monitoring system to keep it up and running. You can't find quieter, faster and more reliable service. And since it is digital, it has tremendous **capacity to expand.** That's why we've allocated **$55 million this year** for growth and modernization, and even more in the years to come.

We've made the commitment to provide3 you with the very best service today. And tomorrow.

Tap into the expertise of our professionals.

At Sprint, we realize that the technology is only as good as the people running it. That's why we have more than 1,000 highly trained business, data and video professionals. That includes more than 250 construction, installation and maintenance field technicians and 750 engineering and support professionals serving the needs of the business community alone. We've grouped these

professionals into specialized teams to best respond to your needs and make sure you stay well connected.

10 troubleshooters on line, 24 hours a day.

This is an **immediate response team** specifically serving transmission and fiber optic customers. They are highly trained and ready 24 hours a day.

These experts make up our **Single Point Of Contact** (SPOC) group has access to more than $2 million worth of equipment to expedite, test, dispatch and follow up on any service you need.

Plus, this team interfaces directly with long distance carriers to insure a smooth connection.

65 data and video experts in the field.

Our **data and video field technicians** have more than 30,000 worth of test equipment in each of their trucks. Add to that more than 1200 years combined experience, and you get an equipped and able team ready to isolate and fix just about any problem on the spot.

As if that weren't enough, we also arm them 10,000 hours of new training every year.

20 long distance support professionals working directly with carriers.

These 20 full-time professionals' sole function is to serve all the needs of long distance carriers This commitment of manpower represents our continuing dedication to **a long-term and personal relationship** with long distance carriers. Which translates into a reliable, efficient and seamless **connection to the entire world.**

40 computer technicians monitoring the system.

These specialists oversee two fully-computerized monitoring systems, **24 hours a day.** They use these computer systems to look for trouble in the network

before it happens. In fact, they can spot a problem anywhere in the trunking or switches. More impressively, on of the computer systems even has **specific monitoring alarms** just can isolate and fix it at a moment's notice without interrupting the flow of your calls.

Make sure you're well connected.

At Sprint, we realize that in today's business environment of ever-increasing competition, you cannot risk losing even one call. That's why we've made the investment in technology and people. And why we will continue to do so.
We offer you the very best system available in the valley. And we back it up with the kind of support that only an international communications leader could provide.
For more information, call us at 877-7400, ext. 5. And get **well connected.**

Be there now.

Sprint ® Central Telephone-Nevada
(END BOOKLET)

Sprint
330 South Valley View Boulevard
Las Vegas, NV 89152
Voice 702-244-7171

November 7, 2000

Mr. Eddie Munoz
Computer Consulting and Design
P.O. Box 61344
Las Vegas, NV 89160

Re: Hotel sites for test

Dear Mr. Munoz:

The following is a list of hotels that will allow Sprint to place a PBX technician at the hotel PBX during the test.

Venetian
Aladdin
Sahara
Showboat
Mirage
Bellagio
Treasure Island
Golden Nugget
Palace Station
Sunset Station
Boulder Station
Caesars Palace
Regent Resort (Summerlin)

As we discussed on the conference call, we would like to proceed with the tests on Saturday, November 11,2000, Tuesday, November 14,2000, and Saturday November 18, 2000. Please try and reserve a room at one of the above hotels.

If additional information is required please contact me at 244-7706.

Sincerely,
(s)_____
Scott Collins
Docket Manager-Sprint

...submitted by the parties, pursuant to EDCR 2.15, in support of an in opposition to the Petition.

The Petition came on for hearing before the above-entitled Court, pursuant to NRS 703.373(4), on September 8, 1993, with TODD TOUTON, ESQ. of

LIONEL SAWYER & COLLINS appearing for the Petitioner, and SHELLY T. O'NEILL, ESQ. appearing for the Respondent.

After reviewing the Petition for Judicial Review, and the briefs filed by the parties, along with the complete record of proceedings before the COMMISSION in Docket No. 91-7049, as certified by the COMMISSION's Secretary, and after hearing the arguments of counsel and being fully advised in the premises, and good cause appearing therefore, the Court makes the following Findings of Fact and Conclusions of Law:

FINDINGS OF FACT

I. CENTEL is a provider of telecommunication services in southern Nevada under authority if the COMMISSION. Prior to 1986, CENTEL offered a unique and specialized billing service the major hotels and other customers in Las Vegas. This operator service, called Special Billing Numbers ("SBN"), provided each hotel a designated prefix and allowed the remaining four digits in the telephone number to reflect the hotel room from which a call was placed. CENTEL operators identified the hotel and room via the SBN and then notified the hotel verbally or by teletype of the costs due. This service furnished a hotel with the ability to promptly calculate telephone carges and communicate those costs to hotel guests. Each hotel paid CENTEL monthly for service. Forty-seven hotels subscribed to the service.

II. In 1986 the telephone industry was deregulated and of the operator sevices rendered by CENTEL were shifted to parent company, AMERICAN TELEPHONE and TELEGRAPH (AT&T) it is referred to in the record as a "cutover"/ The 1986 cutover service to AT&T occurred an a gradual basis, a hotel at a *********

10/26/00 MAJOR ACCOUNTS - 2000

CUSTOMER	*TELE PHONE #*	*CONTACT NAME*	*ACCOUNT MANAGER*
THE VENETIAN RESORT HOTEL			
SANDS EXPO			
RIVIERA CORPORATION			
RIVIERA HOTEL & CASINO			
FOUR QUEENS HOTEL			
ALADDIN RESORT HOTEL			
IMPERIAL PALACE HOTEL			
SAHARA HOTEL & CASINO			
COAST PROPERTIES			
BARBARY COAST			
SUNCOAST HOTEL			
ORLEANS			
GOLD COAST			
SHOWBOAT HOTEL			
HYATT REGENCY			
TERRIBLE'S HOTEL & CASINO			
SILVERTON HOTEL & CASINO			
LAS VEGAS HILTON (TIMESHARES)			
NEW FRONTIER HOTEL & CASINO			
TROPICANA RESORT & CASINO			
ARIZONA CHARLIE'S			
ARIZONA CHARLIE'S-EAST			
POLO TOWERS			
MONTE CARLO RESORT & CASINO			
STRATOSPHERE TOWER			
MARRIOTT			
LAS VEGAS MARRIOTT			

SUITES			
MARRIOTT RESIDENCE INN-			
ALL LOCATIONS			
COURTYARD BY MARRIOTT-			
ALL LOCATIONS			
MGM GRAND CORPORATION			
MGM GRAND			
MIRAGE			
BELLAGIO			
TREASURE ISLAND			
GOLDEN NUGGET			
GOLDEN NUGGET- Laughlin			
NEW YORK NEW YORK			
PRIMM RESORTS			
MANDALAY BAY RESORTS GROUP			
MANDALAY BAY			
EXCALIBUR			
CIRCUS CIRCUS			
LUXOR LAS VEGAS			
FOUR SEASONS & LAUGHLIN PROP.			
BOYD GAMING CORPORATION			
STARDUST HOTEL			
SAMS TOWN			
MAIN STREET STATION			
FREMONT HOTEL			
CALIFORNIA HOTEL & CASINO			
ELDORADO CASINO			
STATION CASINOS, INC.			
PALACE STATION			
SUNSET STATION			
TEXAS STATION			
BOULDER STATION			
SANTA FE STATION			
FIESTA STATION			

HARRAH'S CORPORATION			
HARRAH'S LAS VEGAS			
RIO SUITES			
HARRAH'S - LAUGHLIN			
PARK PLACE ENTERTAINMENT			
PARIS LAS VEGAS			
CAESAR'S PLACE			
FLAMINGO HILTON			
BALLY'S			
U.S. GOVERNMENT			
DEPARTMENT OF AGRICULTURE			
U.S. ATTORNEY HEADQUARTERS			
U.S. JUSTICE COURTS			
EPA			
FBI			
U.S. POSTAL SERVICE			
IRS			
SOCIAL SECURITY ADMINISTRATION			
REGENT RESORT & CASINO			
VIA WEST			
HARD ROCK HOTEL & CASINO			
HORSESHOE HOTEL & CASINO			
UNION PLAZA			
PLAZA REGENCY			
ATC VANCOM			
CONCENTRIC NETWORK			
SOFTBANK SERVICES GROUP (CLIENT LOGIC)			

Sunday, September 21, 1997

Sprint holding the line on competition

Despite deregulation, the local phone giant has made it tough on newcomers to the Las Vegas market.

By John G. Edwards
Review Journal

The Nevada electric utility industry, which will be deregulated in 2001, can look to the telephone industry for a glimpse of how well competition works in a formerly monopoly industry. But it will find no consensus among the people watching telecommunications deregulation.

After 18 months, telecommunications deregulation impresses some and depresses others in Southern Nevada.

"Its definitely the most competitive market in Sprint's territory," said Richard Pfeifer, Sprint Corp. vice president for finance and regulation.

Lou Emmert, Sprint vice president and general manager, agreed. "In my mind, (competition) has come a lot faster than I expected it."

They count 38 companies approved by the Public Service Commission to provide competitive local exchange services in Nevada. Sprint has interconnection agreements with eight and seven are operating in Southern Nevada.

Fred Schmidt, state consumer advocate for utilities, is disappointed that AT&T Corp. and MCI Communications have yet to start competitive local telephone services in Nevada.

"There's really meaningful local competition yet and people hoped there would be," Schmidt said.

"There's been some positive and some negative," Schmidt explained. "It's too early to say there isn't going to be meaningful competition." But the outlook, he adds, isn't "particularly rosy."

To Neild Montgomery, chief executive officer of MGC Communications, which does business as NevTel,

telephone competition in Nevada has been a hollow promise so far.

His competitive local exchange company must pay more for access to Sprint Corp.'s local network than retail customers of Sprint, the former monopoly company. That may change with a coming decision from the Nevada Public Service Commission, but Montgomery is discouraged it has taken so long for regulators to act.

"No matter what I do I can't compensate for a negative position, " he said.

Another new competitor agrees with Montgomery.

Sprint is "very slow to respond." Said Clark Peterson, vice president and general manger of NextLink, another local telephone exchange. "I think the main issue is their ability to respond quickly to our needs and treat the (competitive local exchange carriers) as fairly as they treat their own customers."

Sprint tells some competitors it can't give them access to some metropolitan areas because it has no available capacity in its facilities, according to Peterson.

"The market is open to competition, and Sprint has accommodated competitors and worked with them.: said Sprint spokesman Vince Alberta.

"There's no way to make money and be competitive in the market when your cost is more than the retail rate," Peterson added.

Sprint Corp. has temporary authority to charge competitors $18.95 for the "unbundled loop" – industry jargon for the last part of lines to customers.

Competitors can try to recover losses and a profit from enhanced features, such as call waiting and forwarding, and long distance to customers, Peterson noted.

The problem doesn't greatly concern NextLink, he said, because probably only 3 percent of his firm's business relies upon paying the wholesale retail for the unbundled loop. NextLink has 460 miles of fiber-optic cable in Las Vegas Valley. NextLink often connects

directly to its customers, but other local phone competitors must rely on Sprint for use of lines to customers.

Rex Knowles, director of regulation and external affairs for NextLink, takes a positive view and treats his contacts at Sprint as partners, rather than adversaries.

"The people in Las Vegas at Sprint Central Telephone have been very cooperative, very good to work with and have been working very hard to work with us and get things do," Knowles said. They are committed to make competition work. We've got problems (but) most of them are process problems."

Still another perspective comes from Steve Sherman, general manager for American Communication Services of Las Vegas Inc. His company has 60 miles of fiber-optic lines and hopes to install its own switch downtown.

ACSI for the moment, however, is a reseller of communications services it buys from Sprint at a 21 percent discount.

In Sherman's worst nightmare, Sprint workers who sell services to him wholesale divulge information about his operations to the Sprint executives who compete with him for retail customers.

Sherman isn't accusing Sprint of disclosing information about his operations with his retail competitors at Sprint, but he can't help wondering.

"That's the scary part," Sherman said.

"Sprint is open to competition, but internally a group is responsible for selling directly to end users. What you're seeing are divisions within Sprint competing against each other."

Montgomery shares those concerns. Sprint has "an ability to determine what the (local) market share is by carrier," NevTel's chief said "No one else in this market would know that."

When the Public Service Commission recently authorized part of Sprint Corp. to compete with Sprint's own local telephone exchange, Montgomery felt the state regulatory body probably had little alternative.

"I think they basically had to approve this application... I don't think they went far enough to establish more specific safeguards."
Montgomery said. "It is rather confusing as to who really is going to be marketing what."

Even more worrisome for some is Sprint's request for regulatory approval to jointly market its local and long distance services, as well as wireless phone service.

Pfeifer, the Sprint vice president, said the company is requesting permission to joint market to existing customers. When new customers call for phone service, Sprint reads a random list of long distance companies. Sprint wants regulators to permit it to add the question: "Or do you want Sprint" long distance?

In October, the Public Utility Commission, a new state regulatory body being spun off from the former PSC, is expected to decide the first phase of the pricing docket for the so-called unbundled loop, the last leg of telephone lines to a customer. The second phase may be completed by year-end, PSC spokesman Rick Hackman said.

"Sprint's proposed rate for the unbundled loop is substantially higher than what will allow us to go in and make competition work," Knowles said.

The proposed rates range from $9.51 in the densest population areas to $53.36 in rural areas, but most areas have proposed rates of less than $22.45. Sprint figures the weighted average is $15.93 under its proposal.

Until the PSC decides the pricing issues, competitors are paying $18.95 for the unbundled loop in addition to the expense of a switch and "transporting" the call, says Kent Heyman, general counsel at NevTel.

Compare that with the $7.10 that Sprint charges residential customers, before federal subscriber line charges and extra features, and the $16.30 it charges for the basic business line before those expenses are added, Heyman says.

If the regulators set prices lower than the current ones, competitors will recover the difference, removing some of the newcomers' cost burden.

Regulators can do little about another advantage Sprint enjoys.

Under the federal telecommunications deregulation act of 1996, the regional Bell telephone companies, must demonstrate their local phone exchange market has become competitive – before they can enter compete for interstate long distance service. The deregulation law provides a 14-point check list for Bell....

APPENDIX M

PGS –A 102-111

P.U.C. DOCKET 00-6057

NATIONAL SECURITY

BATES RECORD 010008
.....PG A-102-104

TERRORIST ISSUES

TRANSCRIPTS OF HEARING 10;
02 AM. MARCH 14, 2002

.....PGS A-105-111

Telephone service lost in robbery

Armed men temporarily knock out phones for about 75,000 valley customers by stealing essential computers

By Peter O'Connell

Review Journal (1-3-98)

Masked men knocked out telephone service Sunday for at least 75,000 customers in southwest Las Vegas when they forced their way into a Sprint telephone office and swiped computer equipment.

Three people were tied up and shot with stun guns during the 8 a.m. robbery at the Sprint office near Spring Mountain Road and Jones Boulevard. Telephone service was resorted by about 3p.m.

Police who reported no arrests by Sunday night, said they could recall no similar heist in Las Vegas.

"They were very specific in what they wanted," Las Vegas police spokesman Steve Meriwether said.

He said a group of three to five men tried using a blowtorch to enter through a rear door of the utility's building. "That didn't work," he said.

Meriwether said the men then went to a front door and knocked. Someone inside the building cracked open the door slightly and the thieves rushed in with handguns and stun guns drawn.

They corralled two men and a woman who were working in the building and tied them up.

"All of them were stunned with a stun gun after they were tied up. One of them was beaten severely," he said.

The injured man was taken to University Medical Center with non-life threatening injuries. His condition was not available Sunday night.

After incapacitating the people inside the building the people inside the building the culprits began removing telephone-related computer equipment.

Sprint spokeswoman Detra Page said the computer hardware was in use at the time it was stolen. Its removal promptly knocked out the telephone service of about 75,000 customers.

Page said she did not know the specific type of equipment taken or its value but she said profit appears to be a motive.

"They (authorities) believe the computer equipment was taken to be resold," she said.

About 90 percent of those who lost telephone service got it back by 1:30 p.m. The remainder got their dial tone back by about 3 p.m.

Page said the Rio and the Gold Coast were among customers who temporarily lost telephone service Sunday.

Southwest Gas spokesman Robert Buehrer said the incident also temporarily prevented residents in the affected areas from placing emergency calls to the company's dispatch center at Arville Street and Tropicana Avenue.

"It could have been more serious, but people used their common sense and called 911," Buehrer said.

With two NFL playoff games televised Sunday, the Domino's Pizza at Spring Mountain Road and Rainbow Boulevard was prepared for a busy day. But the telephone was dead until about 3 p.m. General Manager Fred Brann sent two employees home.

"I got a few orders," Brann said.

Page said all telephone lines in the southwest area of the city go into and out of the office that was robbed Sunday.

The computer theft was detected when workers monitoring telephone traffic at another Sprint office noticed calls were not going through the southwest office.

After police finished their work at the southwest office, Sprint employees determined what equipment was missing and what would be necessary to restore service. The system was not at full operating strength when service initially was restored. Some residents had to dial several times before their calls went through, Page said.

Sprint, which has about 845,000 customers in Southern Nevada, was aware of no similar thefts, Page said.

"We have never had anything like this," she said.□

APPENDIX 10
NATIONAL SECURITY
P.U.C. DOCKET 00-6057
BATES RECORDS
O10008
EXHIBIT 13

BEFORE THE PUBLIC UTILITIES COMMISSION OF NEVADA

-oOo-

EDDIE MUNOZ v. CENTRAL TELEPHONE COMPANY-NEVADA, DBA SPRINT OF NEVADA, Complaint alleging incoming calls are being diverted from customer's business.

Docket No. 00-6057

TRANSCRIPT OF PROCEEDINGS

HEARING
VOLUME 1
10:02 a.m., Thursday
March 14, 2002

Offices of the Public Utilities Commission
Suite 250, Hearing Room
101 Convention Center Drive
Las Vegas, Nevada

Reported by: JERRY J. SILVEN, CCR#55
SILVER STATE COURT REPORTERS (775) 329-6329

(Pages 420-427)
Direct Testimony of Eddie Munoz

A. Yes.
Q. What is it?

A. This is a report that I did on what we did for the testing of 11/14th and 18th of November.

Q. You sent this letter to Miss Uttinger on or about December 21st, 2000?

A. This was in a file. I don't know if it was just actually the letter, but it was in a file.

Q. You did send it to Miss Uttinger, though?

A. Yes.

Q. And at the bottom of the page which has been Bates numbered 010173 you allege that Sprint has – I'll quote you – "just recently did a dog and pony show to comply with the order of the Commission. In the past, Sprint has acted in a acriminal sense in this matter, in their help in the investigations."

Did you say that, sir?

A. Yes.

Q. And you go on to say, and I'll quote you: "Like leading a wolf to" – I believe you mean "slaguheter and a murderer dong his own murder investigation."

A. Yes.

Q. I believe earlier today you stated in your testimony, your live testimony, that Sprint has blocked the investigation of this matter; is that correct?

A. Yes.

Q. Is there anything else you want to add on my colleagues? This is your opportunity, take your best shot.

A. Yes, I would like this very much.

Three days ago, I had discussed the matter of this with Gayland Hammack and Ray Brotherson. I have been working with them extensively, like I've stated.

They were coming to the Commission to give a voluntary statement on the situation of the Las Vegas area; not to back up my testimony in any way. This is, you know, a matter that they've been dealing with for quite a while. And for the president of Sprint to call Jerry Keller and have the officers brought in to find out what was going on, and why the president was more or less reprimanding – I mean, he had the officers brought in. And they explained to him what they were doing, and they

were instructed to tell us that they still want to come and testify, that they were—we just need a subpoena to make everything legal and protocol for the Commission and go by rules and procedures.

And then at that time, from what I understand, the undersheriff, his wife works for Sprint, the DA that wrote that letter yesterday, wife works for Sprint –

Q. Well, can we talk about that letter for a minute?

MR. ALPERT: Excuse me. He's been asked to give an answer and he's been cut off in the middle of his answer.

BY MR. REILLY:

Q. Well, if you have more to say, Mr. Munoz, go ahead and say it.

A. I mean, they worked in this process to enlighten the Commission on the activities that are going on, and about the organized crime that is in Nevada, that this is an existing problem. There is other businesses that they've encountered on this.

Sprint has noted to them that there's no wrongdoing, but there's – they know of other incidents where Sprint has claimed that they haven't been hacked. They've worked on cases and, you know, Sprint's more or less used their corporation power to suppress some of the evidence that could have been presented in this case to enlighten the Commission.

And I think that is—I'm just a little guy, I'm a consumer. It was totally wrong what just happened the other day.

When we go into our rebuttal, it clearly states, its not from my testimony, its from actual Sprint employees and supervisors that were instructed not to talk to me, not to deal with me under any circumstances. That is noted in the trouble tickets.

MR. REILLY: Commissioner, I have a document in my hand, it's a letter from the Office of the District Attorney in Clark County, Nevada, dated March

14th, 2002, addressed to yours truly. I'd like to have it marked as the next exhibit in the record, please.

COMMISSIONER ESCOBAR CHANOS: Do you have copies for everyone?

MR. REILLY: Well, I—

COMMISSIONER ESCOBAR CHANOS: Does everyone have a copy? they should.

MR. REILLY: I think everyone has a copy, we spoke of it yesterday

COMMISSIONER ESCOBAR CHANOS: Mr. Alpert, do you have a copy of this letter?

MR. ALPERT: Yes, I do.

MR. SAUNDERS: That will be marked as Exhibit 21.

(Exhibit 21 was marked for identification.)

MR. REILLY: I'd like to correct that. The letter was sent to the Public Utilities Commission of Nevada. When I said "yours truly" I didn't mean to be referring to me.

BY MR. REILLY:

Q. Mr. Munoz, I'll let you look at my copy if you like.

Mr. Munoz, these two officers that you were referring to are Galand Hammack and Roy Brotherson; correct?

A. Yes, and this is—

Q. These were the two – please focus on the question for a minute.

The two officers who you were attempting to get to testify in this matter were Roy Brotherson and Gayland Hammack; correct?

A. Yes.

MR. ALPERT: Objection. He did not say he was asking them to testify. He testified that they were coming in to make a voluntary statement.

MR. REILLY: Mr. Munoz has answered the question.

BY MR. REILLY:

Q. Mr. Munoz, would you be surprised if I told you that Mr. Brotherson no longer works in the organized crime unit in Las Vegas?

COMMISSIONER ESCOBAR CHANOS: Before we go on, that is overruled. I will allow the testimony to stand. Go ahead.

MR. REILLY: Thank You. I apologize/

BY MR. REILLY:

Q. Mr. Brotherson no longer works in the organized crime unit at the Las Vegas Metropolitan Police Department; correct?

A. The other day he met with me and Gayland, and he expressed about to me about your phone conversation that he had with you. How you were telling him what type of person I was. And he turned around and told you: What's the difference? We're not dealing with that issue. Sprint Donnelly does the exact same thing as I do, publishes a phone book with adult ads. You have 120 adult ads in the phone book.

Q. Mr, Munoz, I asked you if Mr. Brotherson was in the organized crime unit. Is he or is he not?

A. As far as intelligence in Metro organized crime, as far as I know, they're all together. I've been dealing with Ray Brotherson and Gayland Hammack for some time.

Q. Mr. Brotherson is working in the Homeland Security Division of the Metropolitan Police Department since September 11th?

A. The computer task force.

Q. Homeland Security.

A. Well, that's part of their thing, I mean whatever division they transferred –

Q. He's fighting terrorists, not the mob.

A. I understand that. But some of these acts that will be introduced in my rebuttal are about terrorist things. If they can do this to me, they can do this to Las Vegas.

And some of the documents that are going to be presented about the SS7 network that is involving Sprint would allow terrorists to have full access to the

telecommunications in the Las Vegas area and across the United States. And these are issues that he was going to enlighten the Commission about the ongoing lack of security of Sprint.

Q. So this is now a terrorist issue?

A. If they're doing it to me, they can do it to 911 operators and create more havoc in the area.

Incidents that could actually happen with the telecommunications just like when the Sprint robbery happened and they stole the equipment, simultaneously that happened in three other states in the following week where they went into telephone companies and robbed equipment.

Q. Mr. Munoz, you previously filed a complaint with this Commission in 1994, is that right? Is that about the right year?

A. If this is the document that Miss Uttinger gave me.

Q. Well, let me refer you to your direct testimony, answer 2, where you state that you filed CCU-030194-SB; is that correct?

A. I don't have the document in front of me.

Q. Your direct testimony, you don't have –

A. I'm sorry what question are you referring to?

Q. Answer 2. You state in answer 2 that you filed a previous complaint with this Commission, CCU-030194-SB, against Sprint. Is that your testimony?

A. Yes, I filed a complaint – I filed numerous complaints, and I'm not really clear if this is the one your talking about.

Q. Yes, that's the one I'm referring to. That complaint was dismissed by this Commission, wasn't it?

A: The complaint was dismissed because they had—

Q. Simply yes or no, sir. Was it dismissed or was it not?

MS. UTTINGER: I'm going to interpose an objection at this point and make an offer of proof.

Mr. Hackman has informed me that the first complaint never went to the Commission, to clarify the...

48

No. 06-1222 Oct. 30, 2006

In the
Supreme Court of the United States

EDDIE PAUL MUNOZ; PRO SE,
- Petitioner

v.

CENTRAL TELEPHONE
COMPANY NEVADA; ET AL
-Respondents

On Petition for a Writ of Certiorari to the United States Court of Appeals for the 9th Circuit

APPENDIX N-O
VOLUME 2

EDDIE PAUL MUNOZ ; Pro Se
P.O. BOX 61344
LAS VEGAS, NEVADA 89160

APPENDIX N

PGS A-112-133

P.U.C. DOCKET 00-6057

EXPERT WITNESSES

BATES RECORD 005656-008660

KEVIN MITNICK DIRECT TESTIMONY

P.U.C. DIRECT TESTIMONY

RON BARDARSON: EXPERT WITNESS

P.U.C. STAFF

APPENDIX 6
DIRECT TESTIMONY
P.U.C. DOCKET
00-6057
EXHIBIT 43

EDDIE MUNOZ vs. CENTRAL TELEPHONE COMPANY-NEVADA, d/b/a SPRINT OF NEVADA

DOCKET NO. 00-6057
DIRECT TESTIMONY OF KEVIN MITNICK

Mr. Mitnick would you please state your background and expertise in the computer industry regarding the following.

A. Unlawful security breaches (hacking)

B. Information and data security trespasses

C. Related computer security and information technology issues

D. Computer and/or social-engineering fraud prevention

Have you given your advice to agencies public or private regarding these issues and how to prevent future security violations?

Yes I have testified before The Committee on Governmental Affairs United States Senate on the techniques intruders use to compromise computer systems and what steps the Federal Government

Could take to minimize these risks. I am currently writing a book, which will be published by Wiley & Sons on information security issues related to exploiting the human element. I currently host a talk radio show on KFI talk radio in Los Angeles that covers privacy and security issues relating t the internet.

Q1. Is it possible to hack into the Sprint network?

A1. Yes, I was able to do this up until February 15, 1995.

Q2. How did you gain access to the control consoles on Sprint Las Vegas switching systems?

A2. Through dial-up modems Each Nortel DMS switch had an unpublished telephone number, which only required knowledge of a valid username and password.

Q3. How would you access these Nortel DMS switches if it had this unpublished telephone number, username and password?

A3. I would call up RCMAC (Recent Change Memory Authorization Center) posing as a Sprint Employee to have line restored to allow incoming calls. I obtained the default user name and password that Northern Telecom support configured in each switch. The username was: NTAS with a password of HELPER or NTAS

Q4. What would happen after that?

A4. I would have the access to the switch which would allow me to make changes in software that would give me the ability to reroute calls, among other things.

Q5. Were you in the Las Vegas area at the time of the access to the switch?

A5. Sometimes, I recall accessing the south 5 switch from Seattle, WA and Raleigh, NC.

Q6. Were there any other ways to access the Las Vegas Sprint telephone system?

A6. Yes, With a testing system CALRS pronounced "Callers" phone company personnel could run tests on customer lines, "loops" in the parlance of telephony, from a central location. The system consisted of a handful of client computers, and remote servers attached to each of Sprint Central Telephone DMS-100 switches.

Q7. Do you feel that the Las Vegas Sprint-Central servers are well protected from outside access from any source?

A7. No, because they were accessible through low speed dial up modems, guarded by a technique

only slightly more secure that a simple password protection.

Q8. Could you explain in detail how this happened.

A8. The server required the client, normally a computer program, to give the proper response to any of 100 randomly chosen challenges. I would prompt you with a challenge, and you would have to provide the correct response which was based on an internal seed list. For example, the system may issue a challenge of 54, and the proper response may be 3FAE. I recall the response was a 4 hex characters.

Q9. How exactly were you able to get the dial-up numbers information from Vegas Sprint-Centel employees.

A9. It was easy. By conning Sprint employees. I was able to get the "seed list" of challenges and responses from the company that made the system, Ontario-based Northern Telecom, renamed in 1999 to Nortel Networks. All I had to do was call Nortel and have one of the engineers talk me through it. I just told them I was writing software that had to interface with it.

Q10. How were you able to use this system?

A10. It gave me the ability to among other things, silently monitor phone lines or originate and answer phone calls on other subscriber's lines. The only other equipment required was a computer and two phone lines.

Q11. How difficult would it be for an employee to sabotage a business if they were to have access to the systems that were just discussed?

A11. This will be explained in detail when my testing has been completed.

Q12. Are you know investigating the Munoz case with Sprint Centel?

A12. Yes, with the help, of another computer consultant to assist with the computer work required. Mr. Munoz hired Alex Kasper of Nexspace on my recommendation.

Q13. What have you done so far in the investigation?

A13. We have moved Munoz's phone lines to an office in Westwood California to monitor any changes in call volume and to determine the origin of the trouble. Mr. Munoz's calls were answered live and the content of the request was sent to Mr. Munoz's office using the internet.

Q14. What was the purpose of this move of the phone lines?

A14. So that any calls placed to Munoz's telephone numbers would not terminate through Sprint's network. This was for the purpose of determining at what point in the network the calls were being dropped or intentionally diverted somewhere else. We have removed Mr. Munoz's equipment out of the loop to counter any argument that the problem is being caused by customer.

Q15. Have you finished your investigation?

A15. No, at this time we are waiting for more information from the long distance carrier to before we can finish the investigation. So far we have experienced dropped calls and we tend to investigate further. Several complications arose before starting the test. For example, several hotels on the Las Vegas Strip block 866 numbers although the 866 exchange has been around since 1993.

We will then prepare a final written report and supplement this testimony.

Q16. Have you had an opportunity to review any of Munoz's phone trouble ticket provided by Sprint regarding trouble on his phone lines (such as diverted, dropped calls, busies?)

A16. Yes. There is plenty circumstantial evidence, but our investigation has been hampered because Sprint has refused to provide the details needed to decipher the codes necessary to interpret the trouble tickets provided by their office. Sprint's behavior may be intentional to interfere with our investigation of the matter. We have only been

provided with a partial list of the internal codes that have been requested by Munoz. Without the meaning of what the codes man, it is difficult to determine what trouble was found by Sprint technicians.

Q17. Could you explain further in an overview if there a problem?

A17. Sprint has been dragging its feet and been very uncooperative, it wont speak to us and it has only provided a partial list of the internal codes that have been requested by Munoz. Without the meaning of the codes mean, it is not possible to know what trouble was found in the central office and the switch and translation department of the NOC technical assistances group in Kansas City and Las Vegas. Failed to supply us with the proper data reports to draw a conclusion with test results, which hampered our investigation.

VERIFICATION

STATE OF CALIFORNIA)
)ss:
COUNTY OF VENTURA)

KEVIN MITNICK, being first duly sworn, under oath, deposes and says:

That ha has read the forgoing DIRECT TESTIMONY OF KEVIN MITNICK and understands its content and that the same is true of his own knowledge, except for those matters based upon information and belief, and as to those matters, he believes them to be true.

(s)_____
KEVIN MITNICK

SUBSCRIBED AND SWORN to before me this 1st day of November 2001.

(s)_____

NOTARY PUBLIC
RONALD LEVINE
Commission # 1323347
Notary Public- California
Los Angeles County
My Comm. Expires Oct 2, 2003

PUBLIC UTILITIES COMMISSION OF NEVADA
PREPARED DIRECT TESTIMONY OF RON BARDARSON
Docket No. 00-6057

1. **Q. PLEASE STATE YOUR NAME, BUSINESS POSITION, AND ADDRESS.**
A. My name is Ron Bardarson. I am a Staff consultant for this Docket. My correspondence address is P.O. Box 2022, Sparks, Nevada 89432.

2. **Q. DOES ATTACHMENT RB-1 CORRECTLY SET FOR THE YOUR EDUCATIONAL AND OCCUPATIONAL BACKGROUND?**
A. Yes, it does.

3. **WHAT IS THE PURPOSE OF YOUR TESTIMONY?**
A. I am assisting Staff with its analysis of discovery material, the parties' testimony and independently obtained information. I have provided to Staff my knowledge of computer intrusion techniques and best security practices as applied to the telecommunication industry. I am presenting Staff's technical recommendations concerning the complaint filed by Mr. Munoz against Central Telephone Company-Nevada, dba Sprint of Nevada ("Sprint").

4. **Q. WHAT DO YOU RECOMMEND TO THE COMMISSION?**
A. I recommend the following:

The partial review of Sprint's internal security practices begun during this docket should be completed in a separate Staff investigatory docket. Upon completion of a Staff review of Sprint's internal security practices, Staff would file a report with the Commission. Based on that report and any proceedings conducted in that case, the Commission can determine whether or not to order Sprint to conduct an annual security and to file the results of its review, under seal if necessary, with the Commission as a stand alone filing or as part of the "Annual Report" that Sprint makes to the Public Utilites Commission.
The technology available to the average person, including those that would do harm, grows at an astonishing rate. While Sprint has economic incentives to ensure Public Switched Telephone Network ("PSTN") security, the Commission should be informed of Sprint's security measures, as the public would suffer a great harm if breaches occur.

5. **Q. WHAT WAS YOUR MOST RECENT EXPERIENCE THAT WAS APPLICABLE T THIS PARTICULAR CASE?**

A. For four years, I was the system administrator for Intercomm Internet Services, an ISP in Reno. My job duties included working with telephone company personnel provisioning T1/PRI services and network security. Nearly every ill of the Internet occurred at Intercomm, so I have first hand knowledge of a hacker operating within one's network and of security measures necessary to exorcise him. Intercomm also had its share of telephone service problems.

6. **Q. CAN YOU SUMMARIZE YOUR UNDERSTANDING OF MR. MUNOZ' COMPLAINT?**

A. Mr. Munoz' complaint has at least three different aspects. First, a potential problem exists with hotel PBX systems either blocking or

diverting calls some of the time. Next, Mr. Munoz receives incomplete calls, meaning that before Mr. Munoz' operator can begin the handling process the call has been disconnected. Finally, discrepancies are claimed between Sprint's billing and Mr. Munoz' in-house logging. Mr. Munoz claims that the problem must lie within his service provider, as whenever he changes service providers, he experiences an increase in call volume. Mr. Munoz claims that these diverted calls are routed to his competitors.

7. **Q. CAN ANYTHING BE DONE ABOUT THE FIRST ASPECT?**

A. No, hotel PBX systems are independent of Sprint.

8. **Q. CAN YOU COMMENT ON THE SECOND ASPECT?**

A. Yes, although I need to provide a brief overview of the PTSN first.

9. **Q. PLEASE PROVIDE THAT OVERVIEW.**

A. The PSTN has two separate subsystems: 1) the voice network over which people actually talk and, 2) the associated switching network that controls the trunk selection, setup, and takedown. The central component of the Sprint Las Vegas voice network is the DMS-100 switch produced by Nortel. The switching system is composed of a hierarchy of computers, in aggregate known as 'SS7'; also referred to as to as 'out of band signaling'. I considered both systems while evaluating their potential for causing incomplete calls while under the control of a potential hacker. It must be stressed that a hacker is only one of many alternatives that may result in incomplete calls. Incomplete calls can also occur due to incorrect equipment configuration at either Sprint's Central Office end or at Mr. Munoz' Customer Premesis Equipment ("CPE"). Over the course of the years spanning this complaint, faulty equipment or faulty equipment configuration has

been detected and rectified many times. Additional alternatives could include callers with 'cold feet' or indecision over ad selection, cellular phones with insufficient power to complete a call (these calls last about 11 seconds), and kids using 'war dialers' to search for modem lines. ['War dialing' is a term taken from the movie, WAR GAMES, in which a computer uses a modem to dial a pool of telephone numbers].

10. **Q. WHAT DOES THE DMS-100 DO?**

A. The DMS-100 switch controls the translation from phone numbers into the internal Sprint wire numbering system, provides dial tone and ringing signals, and isolates the telephone caller from the SS7 system. It resides within a Central Office building and supplies these services to approximately 100,000 locations. Generally, stories about telephone hackers taking over switches involve DMS-100 or its cousins.

11. **Q. HOW CAN THE DMS-100 CAUSE AN INCOMPLETE CALL WHILE DIVERTING THE CALL TO A COMPETITOR OF MR. MUNOZ?**

A. Generally, it cannot. There is no switch function within the controlling software that first rings one number, waits a few seconds and then sends the call to a second number. The only remote possibly would require that avery sophisticated hacker gain access to the switch software, replace it with modified software while remaining undetected (this routinely does occur on the Internet, it is known as 'rootkiting a box') and then causing this behavior. The big question is why such a sophisticated hacker, who would need sophisticated DMS-100 designer abilities, would be stupid enough to alert Mr. Munoz to the process by first dialing his office.

12. **Q. DO YOU BELIEVE THAT SUCH A HACKER EXISTS?**

A. It is rather unlikely, since hackers love to brag about their exploits. While Mr. Munoz insists that this problem has been going on for years, a story this big would not remain quiet and would eventually show up in underground literature. That literature is online within the Internet; searching it failed to produce any likely candidates.

Mr. Mitnick's direct testimony includes a claim that he achieved access to the DMS-100 regularly until 5 years ago. Sprint has removed his access path. The underground literature shows that Mr. Mitnick's alleged DMS-100 switch hacking was limited to translation table modifications, with which he may have had help. Mr. Mitnick did not respond to a Staff discovery request asking for explicit details on his methods. Nonetheless, I am containing to pursue discussions with Sprint about its internal DMS-100 logging and crosschecking of Sprint security practices to eliminate this possibility, as it may pose a danger to the PSTN beyond merely depriving Mr. Munoz of income. The amount of cash flow within the adult escort industry is sufficient to support such a hacking enterprise and the possibility simply cannot be discarded. If there was a hacker present, he again requires some sophistication, because he has avoided detection during test I will relate shortly.

13. **Q. WHAT ABOUT SIMPLY DROPPING CALLS?**

A. If the DMS-100 switch had a fault that caused dropped incoming calls, Sprint would be overloaded by customer complaints.

14. **Q. HOW WOULD THE SS7 NETWORK FIT IN?**

A. It is even more unlikely that the ss7 is responsible for Mr. Munoz' dropped calls. In reviewing the SS7 switching protocol with an aim to subvert it, I developed a hypothetical spoof that would cause the dropped calls aspect, but without

any diversion. Subsequently, I learned that Sprint maintains an active monitor on the SS7 network. I am following up on the SS7 monitor's capabilities; if they match my assumptions, any such spoofing would be detected if it originated outside of the switches involved in the telephone connection.

15. Q. WHAT KIND OF TESTS HAVE BEEN RUN WITH REGARDS TO INCOMPLETE CALLS?

A. There have been several small or informal tests conducted by Staff individuals. Additionally, while visiting Mr. Munoz to examine his CPE, I counted only 1 incomplete call in the 6-7 that arrived. While these attempts provide helpful information, a more formal test is necessary.

16. Q. WAS A STATISTICALLY SIGNIFICANT TEST CONDUCTED?

A. Yes. Over a year ago, a test was conducted during Comdex. Mr. Collins discusses it within his direct testimony. About 200 calls were eventually placed, all without any failures within the Sprint telephone network. The calls were broken up into groups of about 40 and placed within a very short time. Even a drop rate as low as 10% would have been detected within each of those 40 tests (independent and equal probability for each call). Taken overall, the successful ~ 200 calls imply that any drop rate is less than 3%. With regards to the hacker hypothesis, these results would imply that any phone hacker operating against Mr. Munoz had advanced knowledge of the test and took extensive steps to shut down any diverting network. Even though I would have changed a few things, this testing process was done in a sufficiently appropriate manner and quantity so as to be reliable and dependable.

17. Q. WHAT ABOUT THE CALL LOGGING DISCREPANCIES?

A. My visit to Mr. Munoz's office showed that he has extensive call logging abilities. Afterwards, while reviewing the visit, I realized hat he apparently does not have a central time synchronization ability. Without time synchronization of the various recorders to Sprint time, the effort to crosscheck Sprint logs against Munoz logs becomes enormous and very fallible. Computer clocks are notoriously inaccurate; the cheaper ones drift rather rapidly each day. Additionally, Mr. Munoz had overlooked enabling one of the recorders after completing an adjustment to it several hours before my visit. When he enabled it, it began printing numerous log records, leading me to wonder if the internal buffer had been overwritten while paused, which casts doubt upon the reliability of its log.

18. **Q. DO YOU HAVE ANY RECOMMENDATIONS TO MR. MUNOZ?**

A. With regard to his telephone services, I strongly recommend that he simplify them. The simpler the system, the more reliable. The shorter route between the caller and the Munoz office, the faster the call will provide the caller with a ringing signal – otherwise the caller may hang up thinking the call did not complete. I noticed during my visit that his business calls which are routed to Nexspace and back through Paetec (the long distance provider) too a long time between triggering a call logger and ringing one of the office telephones. It seems that all of his services can be handled within the T1 provided by Sprint. Finally, Mr. Munoz should find out if there is a Small Office service offered by Sprint that includes Sprint supervising his PBX operation. This can dramatically reduce downtime and eliminate finger pointing for logging discrepancies. Mr. Munoz also should rotate any technical help he solicits, in order to find the most competent.

19. **Q DOES MR. MUNOZ' DATA SHOW THAT CHANGING PROVIDERS RESULTS IN INCREASED CALL VOLUME?**

A. No. See Attachment RB-3 for Mr. Munoz' data and RB-4 for my analysis of that data. Mr. Munoz' numbers represent income. My analysis is based on experience, having looked at millions at data points while employed at ESL. Switching providers does not improve Mr. Munoz' income. In fact, during the switch from AT&T to Telco, income dropped by nearly 50%. Note especially that income from the Nexpace provider is rather good.

20. **Q. MR. MUNOZ INCLUDED CALL DROP DATA FROM NEXSPACE IN A RESPONSE TO STAFF DISCOVERY REQUEST 43. DO YOU HAVE ANY COMMENTS ON THAT DATA?**

A. It must be wrong. Mr. Munoz' previous call drop percentage has ranged around 30% by his claim. Mr. Hackman's 9 call test chows that percentage to be high, as does my simple 1 of 6 test. Yet, the analysis of the Nexspace data claims an incredible 80+% drop rate while Mr. Munoz' claims his income has improved! Common sense says that the money is right and the Nexspace analysis is flawed.

21. **Q. IN YOUR OPINION, HAS MR. MUNOZ PROVEN HIS CASE IN THIS COMPLAINT PROCEEDING?**

A. While even a larger customer would have difficulty establishing such a complaint against a telecommunications provider, to date Mr. Munoz has not demonstrated the validity of his complaint against Sprint. Although Mr. Munoz filed voluminous materials with the Commission and provided boxes of additional documents in response to Staff's discovery requests, the documents provided generally refer to incidents of computer (not phone switch) hacking. In the few

instances in which some phone hacking is involved, it is generally rather low-level, not the sophisticated hacking level required to create Mr. Munoz' set of problems.

22. **Q. DID MR. MUNOZ' EMPLOYMENT OF KEVIN MITNICK HELP?**

A. Mr. Munoz' employment of Mr. Mitnick did not clarify the complaint. Even among the cyber underground, Mr. Mitnick is not known to be a phone switch expert. In fact, by moving Mr. Munoz' phone lines, Mr. Mitnick muddied the waters. The idea behind effective troubleshooting is to reduce the number of possible problem sources, not increase it (i.e., Paetec is now a problem candidate, as is Nexspace, and the office which received the calls, etc.). Mr., Mitnick's skills are definitely in "social engineering", effectively leading a targeted person to make a desired action based on his allusion.

The choice of Mr. Mitnick immediately shifted Sprint into an adversarial position because of Mr. Mitnick's skills and history. Mr. Munoz' daily logs show that additional Sprint help disappeared. That assistance was beyond the normal service level I ever received, despite having many times the volume and billing with my provider, Attachment RB-5. While Mr. Munoz gained some press notoriety with Mr. Mitnick and, perhaps, gained some credibility with a hacker hypothesis, I have not seen anything from Mr. Mitnick that increases my belief. A technical analyst that simply thoroughly examined Mr. Munoz' CPE, and worked with Sprint to resolve problems, while crosschecking everything, could have provided a rock solid foundation for his case, should there indeed be some problem beyond Mr. Munoz' CPE.

23. **Q. WHY ARE YOU INVESTIGATING THE HACKER POSSIBILITY SINCE YOU HAVE**

MENTIONED THAT IT IS RATHER LOW PROBABILITY?

A. Thinking about the probability of occurrence is the wrong viewpoint. My training tells me that the correct viewpoint is the damage cost such a probability has versus the cost of some small effort to further reduce a low probability. The damage cost far outweighs the cost of a through review.

24. **Q. SHOULDN'T SPRINT BE CONDUCTING SUCH A REVIEW?**

A. I think so, however, while I have encountered several capable Sprint employees, each an excellent specialist, some have clearly never considered the presence of a sophisticated hacker, the kind routinely found on the Internet nowadays. Additionally, I have not yet encountered anyone thinking about "breaking into your own system", which is the best way to improve a system's security. If such a person exists, I cannot help wondering why she/he is not a witness in this docket..

25. **Q. IS IT POSSIBLE TO RULE OUT A HACKER WITHIN THE SPRINT SYSTEM?**

A. Based on my review of the materials submitted, no. To explain this, I need to spend some time discussing the never ending game between 'white hats' and 'black hats'. For instance, scrambling satellite TV signals was once performed with ViedoCypher I. This scrambling system was broken and pirate descramblers were widely deployed. The 'white hats' developed and touted VideoCypher II. The 'black hats' broke VideoCypher II faster than VideoCypher I, because of the education they had received during their initial efforts and because the more complex a system becomes, the more likely someone may introduce a weakness. While at ESL, we developed surveillance systems to intercept drug-related radio traffic. The 'black hats' switched to

frequency hopping radios; we broke the radio hope sequence. Once again the other side upgraded their technology and once again we detected and devised ways of beating this upgrade. Each side had a strong purpose behind their efforts and the introduction of new technology by the other side did not deter that purpose.

There are many such examples, but as a general rule the secure lifetime of any new system introduced by one set of 'hats' grows shorter as the other set of "hats" has become educated from previous efforts and because of the possibility of a complexity weakness. In examples where a new system was introduced that survived much longer than might be expected from said rule of thumb, it is because the time was spent attempting to 'break into your own system'. Surprisingly, another reason why a system is more resilient, is that it is openly discussed.

26. **Q. CAN YOU RELATE THIS TO THE PHONE SYSTEM?**

A. Many years ago, telephone call switching was performed 'in-band', meaning that the switching signals were within the audio passband for the voice conversation. Piecing together snippets of information gathered from the phone company, groups of phone hackers were eventually able to place free phone calls and occasionally mislead attempts to trace them. Eventually, the switching was moved to the SS7 system, and most phone cloning demonstrated.

Within the adult entertainment industry, more than sufficient financial rewards are available to provide a purpose. This is not the only group of people that might have a desire to obtain switch access. The existence of many Internet incidents demonstrate that hackers are twiddling their thumbs and telling stories of the old days.

27. Q. IS THERE A PARTICULAR AREA TO EXAMINE?

A. A very major difference between the Internet and the phone system is that of access. The Internet provides roughly equal access; every point of the system can contact every other point. The phone system provides divided access; consumers are separated from switching. This does a pretty good job of blocking hackers. However, these switches are complex devices in constant demand and cannot be allowed even the shortest down time. Therefore, switches have inherent (and required) backdoors, in order to ensure minimal downtime. The fiber network that connect the switches carry multiple signals simultaneously. While fiber lines can be tapped and the signals demultiplexed, this access point is detectable.

The DMS-100 switch backdoor is via a modem line guarded by a challenge-response password system. A similar backdoor probably exists inside SS7 computers. Thus, the switches should be examined first.

28. Q. THIS STILL SEEMS PRETTY EXTREME. CAN YOU PROVIDE MORE DETAIL?

A. Certainly. While on tour of a Sprint Central office, I noticed a Windows computer in the area of the SS7 control console. It is most likely present to provide email to the operator. Because of the authority of Staff, I was able to learn the name of a switch operator a few minutes later. These two bits of information, a Windows computer for mail colocated with the switch and an operator name could have been obtained in many, many ways.

Assuming I am a potential hacker, I could easily perform some basic detective work and similarly locate a switch operator, eventually finding a way to meet him or her. With some research and some quick wits, I could establish a common interest

with the switch operator. For instance, he is a fight fan and I work for a company that gets extra tickets, or she is a chess player and I suggest a correspondence game after a quick skittles game. My sole purpose is to get an email address and leave an expectation that I will send something important. All of the above is basic social engineering, as described by Mr. Mitnick during his weekly radio shows.

I could then send an email to that Windows computer in the SS7 area with a specially crafted enclosure designed to give me full remote access to the computer. Perhaps, Sprint Internet security prevents reception of email with enclosures. I counter with a website link that downloads the same package. During the night, I stroll through the Windows computer looking for useful clues. Perhaps the challenge-response algorithm controlling access to the modem line is S/key and the Windows version of the S/key calculator is installed on that computer—I get the switch access codes. Perhaps an internal memo has been distributed, printed and then deleted that contained mention of some of the switch access codes. I dig it out of the Recycle Bin and use the samples to crack the algorithm and generate future keys. Or, perhaps I scan the unused areas of the hard disk looking for clues. Finding nothing, I investigate the email to find other people to try next.

Having access to a single computer and its email, I can spread to other Windows computers simply by pretending to be internal email. Eventually, I might encounter some way into the DMS-100 or SS7 backdoor. One of the surprising features of this attack is that the higher one progresses into the company hierarchy, the easier the process becomes, unless there is a strongly enforced security policy WITH crosschecking. With

independent monitoring of the backdoors, any such hacker would eventually trip an alarm. All of the steps in the proceeding paragraphs have been possible for several years. More importantly, such hacking was VERY easy to accomplish shortly after company email was mandated. Nor is such hacking far-fetched for a certain crowd of people, whole presence is not in doubt as they are constantly making new headlines. Las Vegas is the usual site of DEFCON, an annual hacker convention, so there is probably someone knocking on the door; whether they can do more than that is the question.

29. **Q. WHAT IS YOUR CONCLUSION TO THE COMMISSION?**

A. The best result for the Nevada consumers from this case would be the completion of a Staff internal security review in a separate investigatory docket and, if ordered by the Commission, establishment of an annual report from Sprint to the PUC regarding Sprint's ongoing security audit. If the specter that Mr. Munoz raises does indeed exist, there are rather disturbing consequences. It would be better to rule out the possibility than suffer them.

QUALIFICATIONS AND EXPERIENCE OF RON BARDARSON

EDUCATION

1975-1977	United States Naval Academy, Physics minor.
1977-1979	University of California, Bachelor of Science in Physics, with honors.
1979-1982	States Univ. of New York, Graduate work in Nuclear and Astrophysics.

WORK EXPERIENCE

2001 to Present — Independent Consultant

1997-2000 — System Administrator
Intercomm Internet Services

System Administrator for Intercomm, a 24/7 operation, thus system stability is a critical factor. Their network is composed of a dozen special and general purpose computers; a mix of Solaris, Cisco and WinNT systems, serving over 2000 users. Devised a tape backup system supplemented by a daily backup to a spare disk. Instituted a paper trail for system configuration changes. Numerous script tools written for support staff and for investigative troubleshooting . Installed Solaris on new hardware and initial tuning of configuration. Developed method of IP transfer without loss of connectivity. Created scheme for virtual IPs housing common services to allow for hardware changes without loss of service.

1984-1996 — Staff Engineer/Scientist,
Direction Finding System,
TRW SIG (formerly ESL).

ESL specialized in high performance, low volume defense systems. While working on a Direction Finding project, my effort staged through: paper design, computer verification, initial anechoic chamber scale modeling, statistical data analysis, subsystem hardware support, antenna test, system test & integration in the anechoic chamber, and flight test (for airborne

versions). Customer presentations were common, as were test plans, capital equipment planning, and budget reviews. Directed technicians and engineers for eleven years. Assistant Project Manager with oversight for $2M budgets and 3-6 member teams for five years. Participated in TRW Management Training Program.

APPENDIX O

PGS 134-162

P.U.C. DOCKET 00-6057

CLOSING ARGUMENTS OF
EDDIE MUNOZ AUG-16-2002

P.U.C. DOCKET REBUTTAL
TESTIMONY OF SCOTT COLLINS

REBUTTAL TESTIMONY FROM
EDDIE MUNOZ

APPENDIX 8
IN
P.U.C. DOCKET
00-6057
CLOSEING ARGUMENT
FILED AUG 16, 2002

CLOSING ARGUMENT OF EDDIE MUNOZ

Complainant Eddie ("Munoz"), by his attorney, PETER ALPERT, ESQ., respectfully submits his written Closing Argument

A. **Summary of case history.** Munoz has operated several businesses in Clark County for many years. In 1992, Munoz filed a complaint with the F.B.I. alleging that his incoming telephone calls routed through Sprint's network were being diverted. (Transcript, Volume 2, p.301, line 4 to p. 302, line 4.) Munoz also filed complaints with the F.C.C. (Tr., V . 2, p. 305, 1. 24 to p. 306, 1.9.) Other complaints of diverted telephone calls were made directly to Sprint. (Tr., V. 2, p. 306, 11. 13-23.) In February, 1994, Munoz filed a similar complaint with the Nevada Public Utilities Commission ("Commission"). (Tr., V. 2, p. 360, 11. 12-25.) None of the above complaints filed by Munoz resulted in a finding as to why his telephone calls were not being received.

After numerous subsequent contacts with Sprint regarding the same diversion problem and with no progress towards a solution, Munoz filed a Verified Petition for Alternative Writ of Mandate on April 11, 1999 in the Eighth Judicial District Court in Las Vegas, Nevada (Case No. A401763) seeking to have the Commission investigate his numerous complaints and to hold a public hearing. The case was dismissed voluntarily by Munoz on April 29, 1999 after the Commission agreed to open a file and pursue this matter. After one year of delay on the part of the Commission, Munoz filed a second Verified Petition for Alternative Writ of Mandate on May 19, 2000

(Case No. A419237), which precipitated the proceedings that culminated with the formal hearing in this matter.

B. **Burden of proof.** At the outset of these proceedings, the Commission informed Munoz that he had the burden of proof regarding his allegations of phone diversion and/or blocking of calls. For several reasons, placing the burden of proof on Munoz was not realistic nor was it a practical means of determining the cause of the problems raised by this docket.

1. All of the network phone lines, switches and other transmission equipment for the delivery of telephone calls to Munoz are controlled by Sprint and Munoz has no access to them for the purpose of performing testing procedures.

2. Munoz is a small businessman who does not have the financial capability of funding the type of testing required to determine where the problem lies, even if he did have access to the Sprint network.

3. Much of the information requested from Sprint by Munoz during the discovery process was deemed by Sprint to be either proprietary, subject to the attorney-client privilege or destroyed, thereby further hampering Munoz's ability to determine the cause of his problems. Despite these roadblocks, Munoz's efforts in this case led to the discovery of the following facts:

a. Several other persons and businesses experienced problems during the 1990's similar to those experienced by Munoz and they filed complaints with Sprint, the Commission and various other agencies. See, i.e., Exhibits 1-5. Rick Hackman, in his Direct Testimony, stated that he saw a pattern in these complaints and that "it seemed more than a coincidence." See Exhibit 53, Q&A 17.

b. The Commission's Staff opined at various times "that something weird was going on" and that "there has got to be something going on here" based on the complaints of diverted/blocked calls received by the Commission. See Exhibit 56.

c. In Kevin Mitnick's Direct Testimony, he opined that "there is plenty of circumstantial evidence, but our

investigation has been hampered because Sprint has refused to provide the details needed to decipher the codes necessary to interpret the trouble ticket reports provided by their office." (Exhibit 43, Q&A 16.) This allegation was not rebutted by Sprint at the formal hearing.

d. Staff's own consultant, Ron Bardarson, in responding to a question about the existence of a hacker in the Sprint system, stated that . . . "the possibility cannot be discarded." (Exhibit 7, Q&A 12.)

e. Scott Collins, Sprint's Docket Manager, in his Direct Testimony, stated as follows:
"He (Munoz) has shown me enough circumstantial evidence to convince me that he believes he is not receiving his c alls from hotel rooms. (Exhibit 42, Q&A, p. 8, lines 17-22.)

Looking at the overall picture painted by the above examples, it is respectfully suggested that Munoz has come upon a flaw in Sprint's system's which only Sprint is capable of detecting since only it has access to the network. Perhaps the age-old adage is applicable to this case: "Where there's smoke there's fire,"

C. Munoz's investigative efforts.

1. **The Holtz Group ("Holtz".)** Munoz retained Holtz in 1996 to investigate his phone problems. While Holtz did perform some testing, it had no access to Sprint's network and it received improper reports. Therefore, Holtz could only attempt to replicate Munoz's problems and speculate as to possible underlying causes. Holtz's reports are in evidence as Exhibits 30,31 and 40. As a part of the Holtz report, the possibility of a technical problem within Munoz's equipment was raised. (Exhibit 30, p. 5, sec. III A.) However, Munoz testified that Amtec consistently monitored his equipment and never found any defects in the equipment. (Tr. V. 3,pp. 491-494; also Exhibit 39.) After eliminating Munoz's equipment as a culprit, neither Holtz nor any of the other experts retained by the parties have been able to give a definitive answer why Munoz is not receiving his phone calls.

2. **November, 2000 testing.** Exhibit 37 is a summary of the phone calls made during November, 2000 as a result of testing performed by sprint after coordinating the format for the testing with Munoz and the Commission. The evidence shows that of 472 calls made during the test period only 271 were received by Munoz. In Scott Collins' own handwriting he acknowledges in Exhibit 37 that 201 calls are "missing." During his testimony on June 27,2002, Mr. Collins, after the passage of 19 months since the testing in November,2000, tried to verbally change what the written document undeniably shows in his own handwriting to instead mean that "there was a difference of 201 calls", not 201 calls missing. (Tr., V. 4, p. 775, 11. 10-17.) The undisputed fact is that there has never been a reasonable explanation by Sprint as to what happened to these 201 calls, a circumstance which clearly supports Munoz's allegations that he has not been receiving all of his phone calls. One page of the Sprint Special Request Report, included as part of Exhibit 37, shows nine (9) calls made to Munoz from Las Vegas hotels with a call duration of "0." Mr. Collins' explanation of this phenomenon, **which we heard for the first time during his testimony on June 24, 2002,** just does not make sense. In order to reconcile the "difference of 201 calls", Mr. Collins arbitrarily opted to exclude all calls of less than ten (10) seconds that were reflected on the SMRD. (Tr., V. 4, p. 780, 11. 11-16.) However, this begs the crucial question in this docket: What happened with those calls? An answer to that question would solve the continuing mystery. The calls obviously got through the hotels' switchboards as they are reflected on the report tracking the calls at Munoz's end. It is respectfully suggested that Sprint either has no answer or it is not disclosing all that it knows about this problem. See sec. D.8 below for further discussion of Sprint's failure to offer any technical expertise in this docket. Further, Sprint personnel were instructed not to discuss Munoz's phone problems with him due to ongoing legal problems, etc. (Exhibit 47 , pp. 010684, 010706, 010708-9.)

3. **Rio Hotel incident.** Munoz testified regarding a documented telephone call made to his number on January 5, 2001 from the Rio Hotel which he never received. (Tr., V. 2, pp. 445-449.) The calls to Munoz from the Rio were diverted to a number in California. Although someone appeared at the customer's room at the Rio in response to the call to Munoz, that person was not sent by Munoz and one can only speculate how that person knew where to ho at the Rio. Again what happened to the call?

4. **Kevin Mitnick.** The Commission is familiar with Mr. Mitnick's background and qualifications so they will not be repeated this time.

Mitnick was retained to perform extensive testing to determine the reason(s) for Munoz's diverted/dropped phone calls. His Direct Testimony (Exhibit 43), as well as his testimony before the Commission on June 24, 2002, which was for the most part unrebutted, can be summarized as follow:

a. Mitnick was able to gain unauthorized access into Sprint's Nevada network by using dial-up-modems on multiple occasions from 1993 – 1995, none of which were detected by Sprint. (Tr. V. 4, pp.618-623; p. 652, 1. 8 to p. 654, 1. 17.) Sprint cannot rebut this as it destroys its switch logs within forty-eight (48) hours. (Tr., V. 4, 0. 719, 1. 23 to p. 720, 1. 14.)

b. Mitnick, with the assistance of Nexspace, moved Munoz's phone lines to Westwood, California so all calls placed to Munoz's phone numbers would not terminate through Sprint's network. **This procedure also removed Munoz's own equipment as a culprit for the diverted/dropped phone calls.** (Tr. V. 4, pp. 637-640.)

c. Mitnick's review of Sprint's trouble tickets was hampered due to the lack of information regarding the codes used by Sprint. (Tr., V. 4, p. 641, 11. 2-7; p. 682, 1. 18 to p. 683, 1. 13.)

d. Munoz was not able to adequately fund the testing that Mitnick had planned to do. (Tr. V. 4, p. 638. 11. 9-10.)

e. Mitnick did not have access to Sprints network and internal switches for purposes of performing his recommended testing. (Tr., V. 4, p. 640, 11. 2-18.)

f. Mitnick recommended that any additional testing would
have to be performed with Sprint's full cooperation as open access is required to Sprint's network and switches. (Tr., V. 4, p. 640.)

Mitnick referred in his testimony to a "seed list", which contained the challenges and responses devised by Nortel in order to obtain the dial-up numbers to access Sprint's system. This list was produced during the hearing and was admitted as Exhibit 52. This document corroborates Mitnick's testimony that he was able to compromise Sprint's network on numerous occasions.

5. **Bridged taps.** Munoz found 2 bridged taps on his phone lines (Tr. V. 5, pp. 891-894.) He also discovered that someone had a test line programmed into his T-1 circuit from another location without this knowledge. (Tr. V. 5, pl 893, 11. 12-22.) Mr. Collins testified that a bridged tap may cause crosstalk and static on a DS1 circuit. (Exhibit 42, p. 7, 11. 8-14.)

6. **Trouble tickets.** Exhibit 47 contains more than 100 pages of "trouble tickers", which are repair records maintained by Sprint. All of these trouble tickets contain problems Munoz experienced over a long period of time relating to switches, Sprint's Central office, translations, trunks and the testing of his T-1 circuit. All of these documents were produced during discovery.

D. **What have these proceedings accomplished?** The burden of proof issue has been discussed above. IN attempting to satisfy his burden of proof, Munoz has been successful, at a great personal and financial expense, in shedding light on numerous issues which the Commission may consider on rendering its decision in this matter:

1. Sprint's Las Vegas network has been compromised in the past and, in Mitnick's opinion, can still be compromised.

2. The phone problems being experienced by Munoz have also been experienced by several other business.

3. Sprint has been less than prompt and forthright in giving full and complete responses to discovery requests, particularly explanations of alpha and numeric codes on trouble tickets. It also destroys certain business records in a peculiarly short period of time, thereby eliminating any audit trail.

4. The "testing" performed by Sprint has either not replaced the phone calls made from hotel rooms (i.e., they were made from lobby phones) or there was such a large unexplained discrepancy between the test calls made from hotel rooms and those received by Munoz that no satisfactory conclusions were ever communicated to Munoz.

5. Numerous law enforcement agencies, including the Las Vegas Metropolitan Police Department, the federal Bureau of Investigation and the Nevada Attorney General's Office have investigated and/or are still investigating Munoz's complaints of diverted/blocked calls.

6. The issues set forth in Munoz's formal complaint also have implications concerning national security as a result of the ability of hackers to compromise telephone company systems. (Tr.V.4,p.669,l.24 to p. 671,l.2.)

7. Sprint has offered no evidence at the formal hearing that it has performed an exhaustive test of both its network and Munoz's system in order to reach a final and determinative conclusion regarding Munoz's complaints.

8. All of Sprint's discovery responses were prepared by Scott Collins, Sprint Docket Manager, as was all of Sprint's testimony at the formal hearing presented by Mr. Collins, although the issues in this docket are very technical in nature. Mr. Collins admittedly has no technical expertise in these matters. This is an issue that was raised by Ron Bardarson in his Direct Testimony. It is apparent from Mr. Bardarson's Direct Testimony that the Sprint personnel he dealt with never considered the presence of a sophisticated hacker nor did he encounter anyone at Sprint who gave any thought to breaking into its own system as a test of its own security system. With all of Sprint's expertise in the telecommunications field, not

one person with technical telecommunications knowledge was presented to explain to the Commission what was happening to Munoz's phone calls. (Exhibit 7, Q&A 24.) Both Munoz and the Commission retained experts in an as yet futile effort to resolve this docket's issues. It does indeed seem very odd that Sprint, with all of its telecommunications expertise, chose to offer no technical explanations to the Commission other than what Mr. Collins may have Mr. Collins may have heard from co-workers. If anyone could get to the bottom of this docket's issues, it is Sprint as it has complete control of the network and it should have the personnel who are trained to operate and secure the network.

E. What is the appropriate remedy? After exchanging thousands of documents during the discovery process and listening to testimony for almost five full days, it seems apparent that no one individual telephone user is going to be able to determine the source of Munoz's and other users' phone problems without a complete and exhaustive study of Sprint's network by persons and/or entities having full access to everything and everyone necessary to conduct such a study.

As noted previously to the chagrin of Ron Bardarson, Sprint offered no technical explanations or alternatives to explain Munoz's dilemma other than to blame the problem on his equipment or alternatives to explain Munoz's dilemma other than to blame the problem on his equipment and advertising. While these factors admittedly need to be ruled out, the Nexspace testing took Munoz S equipment out of contention as a culprit as well as did the Amtec service agreement which resulted in constant monitoring of the subject equipment. The advertising theory initially raised by Holtz was also appropriately addressed by Munoz, who has spent tens of thousands of dollars on targeted ads, changed telephone numbers and enlarging his distribution network or news racks throughout Clark County and the City of Las Vegas. Munoz has not sat on his hands- he has made necessary changes based on opinion given to him. Unfortunately, he

never received a through and unbiased review and/or opinion for Sprint.

On the other hand, both Munoz and the Commission presented evidence from persons with high levels of expertise in the telecommunications field, albeit with differing points of view. Each of them, however came to the same conclusion; i.e. additional testing is required if the issue before the Commission is going to be resolved. It is also important to keep in mind that this is not a "Munoz" issue. The problems discussed in this docket have been experienced by numerous others and the ultimate ramifications if these problems are not resolved "are rather disturbing." (Exhibit 7, Q&A 29.) A summary of the recommendations made by the experts in this case follows:

1. Mitnick

a. An originating trap and trace should be set up in each of Sprint's central offices in the Las Vegas area. This would enable audit records to be created, which could be compared to the records of the long-distance carrier. (Tr., V. 4,p. 640, II. 8-18.) Sprint declined this request.

b. An ss-7 trap and trace should be set up with a long-distance carrier to determine if there is any manipulation happening over the network. (Tr., V.4,p.640, II. 19-25.)

c. There is something "amiss" in that Munoz is not receiving his calls and more testing of Sprint's network is required. (Tr., V.4, p. 657,1. 16 to p.659,1.9.)

2. Bardarson. Mr. Bardarson testified at length regarding the testing he would recommend in this case. He also opined that the Commission's Staff should complete an internal security review in a separate investigatory docket. (Exhibit 7, Q&A 29.) On cross-examination on June 25, 2002, Mr. Bardarson gave the following testimony regarding the additional testing he would do in attempt to resolve the issues raised by this docket:

Q (Mr. Alpert) You also testified that the testing should be done for an extended period of time. What do you consider to be an extended period of time?

A Given Mr. Munoz's sort of period of complaint, I would strongly suspect that two weeks is sufficient. You may be able to do it in less.

Q This is a two-week continuous testing?

A Twenty-four hours a day.

Q Who would suggest conduct the testing?

A Well, I'm a very hands-on kind of person. I can expound upon my background where there's a few legends about my troubleshooting ability. I would be interested in doing that. But I'd want to ensure that I had carte blanche.

In the past I've been given that and I've done quite remarkable things. There are other people that are available. I don't necessarily want to do that, but I do have a different point of view here.

Q What do you mean you have a different point of view?

A Well, I'm quite willing to listen to what Mr. Munoz says, even though at times I wonder whether or not it's fully going on, I'm quite willing to listen to what Sprint says. And I believe that they could both be exactly right.

You don't know what's really going on here until you sit down and go through that detailed test and you carefully dot your I's and cross your T's time after time, you don't really know. You can't rely on a human being to do that. You need to machine logging, and you need to do that in a fashion that both sides can come to agreement on.

I happen to be sitting in the middle of both sides.

Q Have you performed this type of testing before?

A I've performed very similar testing on thousands of data points while working at ESL. That was one of my primary troubleshooting techniques. Its not thousands, it's probably in the order if millions, carefully indicate evaluating the data in both places.

To give you a small story of the kind of abilities I had – of the kind of power I had at ESL, I've been known to be sent to a site to a site where people had been working on a problem for three days, and walk in and

solve the problem in 20 minutes. And that's not because I have some extraordinary ability other that the fact that I'm willing to think outside the bounds that everybody else wants to put on the problem.

It's very simple for me to reach over an say: You guys never considered this. I consider all possibilities and try to keep the field open as much as possible. I also protect people's confidentiality. (Tr., V. 5, pp. 864-866.)

It is apparent from Mr. Bardarson's extensive exposure to this docket that he is familiar with the respective positions of Munoz, Sprint and the Commission and that he is in a position, with the cooperative of all parties, to use his best efforts to once and for all reach a definitive answer to a question that has eluded everyone for many years.

F. **Conclusion.** There is nothing more that Munoz can do the prove his case. The answer lies in more testing and the experts are in agreement on this. To have come this far only to fail to resolve to issues raised by Munoz will result in financial ruin by Munoz and could potentially have far-reaching national security and organized crime implications.

It is respectfully requested that the Commission order the parties to cooperate and jointly conduct such futher testing as Mr. Bardarson or another Commission designee deems appropriate and that the Commission retain jurisdiction of this docket until such testing has been completed, a final written report has been prepared ad submitted to the Commission and the Commission has had an opportunity to fully evaluate the results of the testing.

DATED: August 14,2002.

(s)_____

PETER ALPERT, ESQ.
State Bar No. 3488
2950 East Rochelle Avenue
Las Vegas, Nevada 89121
(702) 866-6155
Attroney for EDDIE MUNOZ

CERTIFICATE OF MAILING

I hereby certify that on August 16 2002, I sent a copy of the foregoing CLOSING ARGUMENT OF EDDIE MUNOZ, by regular First Class Mail, postage prepaid, addresses to the following:

Louise Uttinger, Esq.
Public Utilities Commission of Nevada
1150 East William Street
Carson City , Nevada 89701
Attorney for PUC Staff

Rick Hackman
Manager, Consumer Complaint
Resolution Division
1150 East William Street
Carson City , Nevada 89701

Patrick Reilly, Esq.
Hale Lane Peek Dennison
Howard and Anderson
2300 West Sahara Ave., 8th Flr., Box 8
Las Vegas, Nevada 89102
Attorneys for Sprint

Richard Hinkley, Esq.
Public Utilities Commission of Nevada
101 Convention Center Dr., #250
Las Vegas, Nevada 89109
Attorney for PUC

(s)_____
An employee of Peter Alpert, Esq.

PUBLIC UTILITIES COMMISSION OF NEVADA
REBUTTAL TO PREPARED TESTIMONY OF
SCOTT COLLINS
REBUTTAL TESTIMONY FROM EDDIE MUNOZ
Docket No. 00-6057

(RECEIVED
FEB 28 2002
PUBLIC UTILITIES COMMISSION
LAS VEGAS)

1.Q. Please state your name and address.

1.A. Eddie Munoz, P.O. Box 61344, Las Vegas, NV 89160.

2.Q. Does Scott Collins Direct Testimony indicate that he has any background in telecommunications security, or that he meets the guidelines set forth in the Nevada Attorney General's Cyber Crime Task Force?

2.A. No. See (Exhibit 1) See (Exhibit 3) Ron Bardarson.

3.Q. Do you have any further comments regarding the testing described by Mr. Collins?

3.A. Yes. See (Exhibit 2) on parameters of test. On the night of November 18, 2000, Scott Collins and I manually counted answered test calls off of the SMRD reports, and he got operation measures reports to get call counts form Sprint switchmen. The discrepancy is very significant due to 201 missing business calls from a total of 406 calls made 205 were test calls. Scott Collins took the results see (Exhibit 3) with him the night of November 18th and was supposed to check what happened during the hours of testing to see why there was such a discrepancy. We only received calls from the test rooms which was very unusual. The only other call received were from cell phones, house phones, long distance and pay phones see (Exhibit 4). This was very strange because reports reflect that hotel guests tried

calling, but didn't get through to us. (exhibit 4) shows the SMRD, hand written notes that correspond to Sprint reports. What did surprise me was that Sprint security took time to identify the trunk groups prior to testing see (Exhibit 5). This explains why we received all calls from test rooms. These calls were made to be sure they went through to us. Sprint had personnel stationed at all points during testing and a few times security would run outside and talk, leaving me in the dark about what was happening see (Exhibit 5). Sprint did not count on the real time data to give me concrete proof of me not receiving any business calls see (Exhibit 4). After Scott Collins viewed these reports at the Commission on February 22, 2000, Sprint had stopped giving reports to me. At the initial installation we had requested on real time data reports to be faxed to me nightly. This service is called Fonview see (Exhibit 7).

4.Q. Mr. Collins stated that none of the test calls were diverted to one of your competitors. Do you agree with that statement?

4.A. I disagree that none of the test calls were diverted. Line 8-Pg. 3: Rio diversion and Rio test see (Exhibit 6). I did follow up with Gayland Hammack and Roy Brotherson of Metro's Organized Crime Bureau about the numbers on the test phone bills see (Exhibit 6-Bates 007349). I had given these numbers to Scott Collins to check out, but didn't get any response regarding the persons associated with these phone numbers. The diversion incident was confirmed from a written statement from a couple at the Rio see (Exhibit 6- Bates 010369). These numbers are in Van Nuys, California see (Exhibit 6-Bates 000606). The bill shows the number dialed from the Rio Hotel room and our office number. On Sprint's bill, it shows (Bates 000613) a Van Nuys

number as in (Exhibit 6-Bates 007349). In Scott Collins deposition, he testified about the Rio diversion and Rio test, but he did not do a report on this diversion incident.

As you can see in (Exhibit 6)(CEN 1530, 1531, 1520, 1521), for their test, Sprint did do a report. We have complained that people get fast busies from hotel rooms. This accounts for origination on reports of callers, being blocked at Sprint's Main. Sprint should have done more investigation on Rio test quick busies see (Exhibit 12F) Ron Bardarson testing. A phone number that went to a pager later came to us, as stated in Scott Collins' deposition (Bates 011393), There are several issues with the Rio that need further investigation. My investigation see (Exhibit 6 – Bates 010397) has led to identifying Sprint switchmen going to the office of Frank Bartello, a competitor. The Rio information is now classified, as it is part of an organized crime investigation.

5.Q. Mr. Collins stated that none of the calls were dropped during the testing process. Do you agree with that statement?

5.A. No. See (Exhibit 4) Scott Collins saw the reports from the November 2000, testing and realized they matched when I showed them to him, that we had 201 dropped calls see (Exhibit 3). After these reports, no data was available to me and Scott Collins talked to my service representatives at Sprint. Within days, Sprint employees stopped taking to me and were transferred. All my customer reports stopped. I have never received any of Fonview reports. Four different Sprint representatives would not return calls see (Exhibit 7). These acts have hampered our investigation and call tracking, which shows we are not receiving our calls. Scott Collins has closed doors by telling everyone this is being handled by "legal", leaving me a consumer with no help.

Service products that were sold to me which were designated for business practices were stopped. These are reflected in (Exhibit 8). Scott Collins also has closed out trouble tickets without permission and with techs not fixing the problems see (Exhibit 15). CEN 84, 98, 2129, 2130, 2132, 2134, 2135, 2136.

6.Q. Do you agree with the reasons for the incomplete calls as described in Attachment B to Mr. Collins Direct Testimony?

6.A. No. Sprint cannot explain 201 dropped calls, quick busies or out-of-service recordings in Attachment B, number 1-800-487-0313 see (Exhibit 9). As you can see, this has nothing to do with porting. This number was on Sprints bills for 3 months 9/24/00, 10/24/00 and 11/24/00 regarding this test number. Why on the night of testing do they get a recording? I have several issues which I have addressed to Scott Collins and his reply is "he'll look into it". We are still waiting for a acceptable response. Sprint wants us to know 205 test calls came through to divert attention from the real issues of 201 missing calls during Comdex, which was attended by 200,000 people and calls were witnessed by Sprint employees. Why did I only receive the 205 test calls? See (Exhibit 3 and 4).

7.Q. Do you agree that the test conducted were valid?

7.A. No. Line 25- Pg.3: It was Sprint's idea to have people stationed at all points of the test, not mine. We should have tested first if there was a problem and been allowed to do more investigation, if necessary. This was a new circuit being used in the test and we should have received all calls, not just the test calls see (Exhibit 10 and Exhibit 4). We were not allowed on a bridge to hear what was happening with Sprint's technicians, who were told to watch what they say around me. See (Exhibit 5).

Line 1-Pg. 4: We weren't invited to the entire test procedure and we didn't get a chance to have our investigator at the Rio do to hotel diversion incidents, See (Exhibit 6).

Line 1-Pg. 4: Sprint Security personnel were using cell phones which are easy to intercept. Hackers are a very sophisticated, elite group of people who can easily access computer and cellular satellite networks.

8.Q. Do you believe that Sprint has taken your allegations of call diversion seriously?

8.A. No. Line 10- Pg. 4 see (Exhibit 8): I have been told by Sprint that it is not a policing agent. Several complaints made by me have been brushed off. Sprint would not cooperate with senior investigators at MCI, AT&T, Telco or Toll fraud units. Switchmen would not respond to weekend complaints at the time of incidents, but waited until Monday morning 9:00 A.M. when things would go back to normal. Weekends are our busiest times and we would get the brush off and insults to our character by Sprint personnel because of the adult aspect of our business. Due to Sprint security's opinion that nothing is wrong, people's time and money have been wasted and lines have been ruined see (Exhibit 11). These acts have been criminal in hampering prosecution, which puzzles me, due to Sprint having over 100 pages of adult ads in the Yellow Pages (owned by Sprint). The three suspects in organized crime investigation own the 100 pages of ads between themselves. See (Exhibits 12 and 13). Yellow page, Representative have been suspended due to involvement of the individuals.

9.Q. Do you agree that Sprint has done a reasonable and prudent job of investigating your complaints?

9.A. No. Line 15- Pg.4: Sprint must have me confused with someone else, since Sprint has only recently done some testing after the Commission allowed a formal complaint to be filed in my case. Since 1996, Sprint and the P.U.C. gave shielded any complaints to be investigated by Sprint telling the P.U.C. that there is nothing wrong. Sprint knows that nobody can test its own network but Sprint see (Exhibit 11 and 14).

Line 17- Pg. 4: Call comparison/201 missing calls see (Exhibit 3 and 4). There is still no logical explanation for these missing calls.

10.Q. Do you agree with Mr. Collins that Sprint has done enough to investigate your claims of call diversion and other service problems?

10.A. No.Line 21- Pg. 4: Since 1996 I hadn't been a Sprint customer until the testing in 2000, so Sprint must be confusing me with someone else for five years and AT&T and MCI Security made complaints to Sprint on my behalf as I was their customer to the F.B.I. and Organized Crime Unit Gayland Hammack and Roy Brotherson.
Line 2- Pg. 2: See (Exhibit 15). Sprint's trouble tickets of T-1 testing circuit show there are various complaints and problems such as framing errors, bio polar variation, two bridge taps, cross talk, etc. There are various network problems. There is little information as to codes and tables, the ability to interrupt properly and the switch and translation problems see (Exhibit 28), are examples of proper codes tables. All of this is located in central offices of Sprint and it isolates NOC technical assistance of Kansas City Nortel switch group. Several times Scott Collins has stopped progress on testing by calling and saying this is being handled by legal network tickets which were classified as proprietary and confidential see (Exhibit 8). We did not get any files from Peggy Barton or the Security Department on these issues. Due to the

lengthy Response to Data Requ8est 47 A-P, we would like to introduce these incidents at the formal hearing.

11.Q. Do you agree with the example given by Mr. Collins on page 4-6 of his Direct Testimony?

11.A. No. Line 1- Pg. 5: See (Exhibit 33), slamming Data Request 47 I.

Line 9-Pg. 5: Federal documents state that Charles Convey has conspired with Sprint employees see (Exhibit 16). This allegation is from the United States Strike Force, Organized Crime, Department of Justice.

Line 17-Pg.28: "These incidents sabotage operators and are very harassing in disrupting business practices. The time and effort to track down telemarketers to stop these disruptions is very difficult.

Line 2-Pg. 6: This beeping sound follows our lines when we change telephone numbers or locations. This sound starts and goes away. It only comes back when something changes with a telephone. It's signal of some tracing equipment, which rings every minute, which is very annoying and scary that people can check coming and going to target a person.

12.Q. Do you agree with Mr. Collins explanation regarding the cross talk problems you have experienced?

12.A. No. Line 7-Pg. 6: See (Exhibit 17). This explains what happened. Bridge tap facts and findings

13.Q. Do you agree with Mr. Collins explanation regarding a bridged tap?

13.A. No. Line 13-Pg. 7: See (Exhibit 17). We had the same problem with another bridge tap had went to the same address- 4212 New York Ave. There was no excessive cable. The office is only six thousand

approximately (6,000) feet from Sprint's 7-E central office. Prior to installation, cable men inspected and tested lines and tagged it a dedicated span line since cable faculties are all Sprint network. How did these taps get placed? Scott Collins states in his deposition that a bridge tap would cause cross talk, static and dropped calls by losing voltage.

14.Q. Do you feel you have provided evidence on how calls are being diverted?

14.A. Yes. Line 18-Pg. 7: I've explained several theories to Scott Collins based on past experiences of problems on a daily basis. He has not produced his notes which correspond with security see (Exhibit 18), or they are now claimed to be confidential and been provided to us. Perhaps this has been inadvertently destroyed too see (Exhibit 31).

Line 19-Pg. 7: Sprint must have me confused with someone else again with similar complaints see (Exhibit 19). This problem is bigger than Sprint wants to admit. If it can't fix the F.B.I.'s phones, what's a consumer supposed to do for help?

15.Q. Do you have the resources or the ability to perform all necessary test in this case?

15.A. No. Line 26-Pg. 7: The entire network is controlled by Sprint see (Exhibit 14). The test during November 2000 gave concrete proof of not receiving all of my hotel calls. The lack of Sprint's cooperation has hampered finding a real solution. My system was end to end with Sprint so we could find the exact source, but I don't have access to Sprint's network systems. A customer is only responsible to DSI unit provided by Sprint.

Line 4-Pg. 8: See (Exhibit 14). For the three days of testing in November 2000, I did excessive advertising and Sprint witnessed my logs and incoming calls. Sprint's

reports show a difference of 201 missing calls. This needs to be explained. I am only a customer trying to run a business. Approximately two hundred (200) pages of trouble tickets shows problems present see (Exhibit 15). See also past trouble tickets see (Exhibit 20). These are all central office issues and switch and translation problems. Frame relays, signaling, trunk groups issues of Sprint network

Line 8-Pg. 8: See reports see (Exhibit 3,4,6,8,15,17). Data request 47 A-P.

16.Q. Do you have any reports that show you are not receiving your calls?

16.A. Yes. Line 21-Pg. 8: The 800 number gives us the origination number of the caller, Sprint's reports show hotel numbers with zero second durtations which us classified as a attempted caller see (Exhibit 21). See circled ingformationj on this report, which shows that the call was not re3ceived. Hotels, monitoring of Sprint NOC of Kansas City states calls from hotels drop. See (Exhibit 21).

17.Q. Do you believe that Sprint is the cause of any decrease in volume of calls to you business?

17.A. Yes. Line 26-Pg. 8: See (Exhibit 3, 4,6,11,15,17,). Line 27 –Pg.8: Sprint has been confused again with someone else. Both Robert Poole and Kathy Hodge testified that is later years they have had several other complaints. See also Rick Hackman testimony see (Exhibit 22).

Line 1-Pg. 9: Sprint's data base does have data that has been withheld from us see (Exhibit 23,29,31) and security files have been destroyed. Sprint Data Basis holds information for years.

Line 5-Pg. 9: Several hundred calls were completed and 201 calls to be exact were dropped and were not successfully completed during the test see (Exhibit 3 and 4). Trouble tickets reflect, thousands f lost calls see (Exhibit 15 and 29).

18.Q. Do you agree with Mr., Collins explanation of Hotel Private Branch Exchanges?

18.A. Line 2-Pg. 10: With 800 numbers, we pay for payphone calls. We pay for all usage and it is free to the customer.

Line 14-Pg. 10: See (Exhibit 24). Consumer complaints of guests in a hotel are to be routed to the FCC and P.U.C. Sprint sells phone systems to hotels manages, (PBXs) see and the hotels control all fiber and COS in the hotel network. See (Exhibit 32). See (Exhibit 7) Ron Bardarson.

19.Q. Do you agree that the P.U.C. had no jurisdiction over private hotel switches?

19.A. No. Line 14-Pg. 10: P.U.C. does have jurisdiction see (Exhibit 24). All aspects of what is occurring in the hotels need to be investigated see (Exhibit 34).

Line 15-Pg. 10: See (Exhibit 34)

20.Q. Have you checked you own telephone equipment to make sure it is working properly?

20.A. Yes. Line 28-Pg. 10: I have checked my equipment thoroughly. The problem is not me equipment see (Exhibit 26). Maintenance logs show no problem.

Line 6-Pg. 11: I have several type of systems from complex to simple. I've had offices with just a phone and a desk. I've had call center of 2000 sq. feet telemarketing set up with 600, 800 toll free numbers. I've had several

locations and problems occur in all if them see (Exhibit 15,29, and 26). The phone system installed by Sprint has had several of the same issues. This is a switch and translations internal problem see (Exhibit 15). SS7 Network see (Exhibit 32).

Line 22-Pg. 11: Kevin Mitnick testimony explained that it was possible to breach Sprint Network. Sprint claims they never had been hacked or had a breach. See (Exhibit 27).

Line 6-Pg. 12: Kevin states he had access until 1995. F.B.I. documents state Organized Crime Bureau figures had access up to 1997. See (Exhibit 16) see (Exhibit 4) Ron Bardarson shows breaches up to 1999.

22.Q. Line 21-Pg. 12: Have you supplied the data re quested by Sprint?

22.A. See (Exhibit 30) 16-32 Data Request Sprints direct questions to investigation of suspects and incidents. I have spent great resource acquiring the data by investigator, surveillance, research, etc. Sprint didn't expect me to have this much information. If Sprint security would have done their job to investigate suspects and claims they might have a better answer than all security files were inadvertently destroyed. So who is wasting who's time 11 years to get someone to stand up and do their hob is criminal.

23.Q. Has Sprint furnished you with everything you have requested?

23. A. No. Line 17-Pg. 12: There are missing security files and traffic reports Sprint should be compelled to produce security files and all related information see (Exhibit 23, 29, and 31 to code tables to understand. Sanction should apply.

STATE OF NEVADA)
)ss:
COUNTY OF CLARK)

Eddie Munoz, being first duly sworn, under oath, deposes and says:

That he has read the foregoing REBUTTAL TO PREPARED DIRECT TESTIMONY OF COLLINS and understands its content, and that the same is true of his own knowledge, except for those matters, he believes them to be true.

(s)_____
EDDIE MUNOZ

SUBSCRIBED AND SWORN TO before me this 27th day of February, 2002

(s)_____
NOTARY PUBLIC

EXHIBITS INDEX

REBUTTAL PREPARED DIRECT TESTIMONY OF SCOTT COLLINS

REBUTTAL FROM EDDIE MUNOZ

Docket No. 00-6057

Exhibit 1 Attorney Generals Office guidelines for protecting citizens

Exhibit 2 Meeting agenda set parameters

Exhibit 3 201 missing calls, deposition transcript, Scott Collins testimony

Exhibit 4 Phone logs and reports of Comdex 11, 14, 18, Hotel SBN numbers

Exhibit 5 Trunk groups, sprint employees stations during Comdex testing

Exhibit 6 Rio diversion statements and facts, Rio test report, Burt Goodrich investigation report

Exhibit 7 Fonview correspondence

Exhibit 8 Audio tape, legal

Exhibit 9 Out of service recording, billing documents

Exhibit 10 Report of 11, 14, 18 Comdex, Sprint reports

Exhibit 11 Staff Rick Hackman testimony

Exhibit 12 News story

Exhibit 13 News stories, New York Times, Review Journal, Metro

Exhibit 14 Staff, PUC, memorandum

Exhibit 15 Trouble tickets

Exhibit 16 Organized crime, Strike force of US attorney office

Exhibit 17 1 Bridge tap, 2nd bridge tap 2nd location

Exhibit 18 Deposition of Scott Collins, Fax to Jerry Franke

Exhibit 19 FBI story on phone problems

Exhibit 20 Past trouble ticket numbers for Telco, MCI and AT&T

Exhibit 21 Sprint report example

Exhibit 22 Staff Rick Hackman testimony

Exhibit 23 Data request denied, destroyed records

Exhibit 24 Jurisdiction PUC and FCC to current legislation

Exhibit 25 Gaming control board

Exhibit 26 Amtec reports and billing, Munoz phone equipmint

Exhibit 27 Kevin Mitnick testimony

Exhibit 28 Example of correct type of code tables

Exhibit 29 Missing data requested from Sprint

Exhibit 30 Index of data request response

Exhibit 31 Missing security and confidential information pertaining to Docket No 00-6057

Exhibit 32 SS7 network vulnerabilities

Exhibit 33 Slamming incident

Exhibit 34 PBX investigation reports

CERTIFICATE OF MAILING

I hereby certify that on the 28th day of February, 2002, I caused to be served a true and correct copy of the foregoing **REBUTTAL TO PREPARED DIRECT TESTIMONY OF SCOTT COLLINS, REBUTTAL TESTIMONY FROM EDDIE MUNOZ,** Docket No. 00-6057, as follows:

Copy with Exhibits to:

Patrick Reilly, Esq.
Hale, Lane, Peek, Dennison, Howard & Anderson
2300 West Sahara Ave., 8th Flr., Box 8
Las Vegas, Nevada 89102
(Hand Delivered)

Louise Uttinger, Esq.
Public Utilities Commission of Nevada
1150 East William Street
Carson City, Nevada 89701
Via Overnite Mail)

Copy without Exhibits to:

Rick Hackman
Public Utilities Commission of Nevada
1150 East William Street
Carson City, Nevada 89701
(Via U.S. First Class Mail)

Richard L. Hinckley, Esq.
Public Utilities Commission of Nevada
101 Convention Center Dr., Ste. 250
Las Vegas, Nevada 89109
(Via U.S. First Class Mail)

(s)_____
EDDIE MUNOZ

(4)

No. 06-1222 Oct. 30, 2006

In the
Supreme Court of the United States

EDDIE PAUL MUNOZ; PRO SE,
- Petitioner

v.

CENTRAL TELEPHONE
COMPANY NEVADA; ET AL
-Respondents

On Petition for a Writ of Certiorari to the United States Court of Appeals for the 9th Circuit

APPENDIX P
VOLUME 3

EDDIE PAUL MUNOZ ; Pro Se
P.O. BOX 61344
LAS VEGAS. NEVADA 89160

APPENDIX P

PGS A – 163- 217

NATIONAL SECURITY

FEDERAL ENVIRONMENT

FEDERAL ARREST

F.B.I. STRIKE FORCE

FEDERAL INVESTIGATION

P.U.C. DOCKET 00-6057

DIVERSION
BATES RECORD 01365-101368

APPENDIX 9
FEDERAL INVOLVEMENT
P.U.C. DOCKET 00-6057
REBUTTAL TESTIMONY
EXHIBIT 4C-4D

Mob Linked to Theft of Call for Dancers
(from: *The New York Times*)
BY: JOHN MARKOFF

LAS VEGAS, Nev., Oct. 15 – in a case of oldest profession meets newest technology, a federal indictment handed up last Friday suggests that the mob is muscling its way into cyberspace.

Federal agents arrested six men here on Oct. 9 after surveillance indicated that the men intended to harm several operators of adult entertainment businesses that openly front for prostitution. Agents stumbled on the plot, the indictment says, because the intended victims were themselves targets of a Federal investigation.

According to the indictment, the men are members of the Gambino crime family who were pressuring a computer expert to divert telephone calls systematically from one or more adult entertainment enterprises to competing companies affiliated with the mob.

Since the mid-1990's, operators of adult entertainment companies known as out-call services have attributed a mysterious decline in business to computer criminals who gain access to the local phone company's switches and illegally reroute calls to competitors.

Although prostitution is illegal in Las Vegas and surrounding Clark County, nude dancing services in which a male or female entertainer is sent to a hotel room are legal. (In some counties in Nevada, prostitution is legal.) Although there are no reliable estimates of the size of the sex industry in this city, the Yellow pages carry 134 pages of advertising in the category of "adult entertainers," one of the directory's largest categories.

Federal officials said that among the six men who were arrested were two mob enforcers who has flown to Las Vegas from Tampa, Fla. They said that the arrests were made after agents became convinced that the lives of several people were at risk.

The two men accused of being enforcers, Vincent Congiusti and Anton Nelsen, came to Las Vegas to threaten three operators of out-call nude dancing services, according to the indictment. The men were arrested when they began looking for Charles Coveney, who is described in the indictment as a computer expert who worked for one of the adult entertainment services.

Mr. Coveney did not return repeated calls requesting comment.

In addition to Mr. Congiusti, 48, and Mr. Nelsen, whose age was not given, agents arrested Christiano DeCarlo, the 27-year-old owner of the DeCarlo Group, an adult entertainment business in Las Vegas; Kenneth Byrnes, 38, described as an enforcer from New Jersey; and Joshua Snellings, 20, of Las Vegas, a driver for Mr. DeCarlo. A sixth man, Mario Stefano, believed to be a Gambino operative, was arrested in New York City on Monday.

The indictment quotes Mr. Stefano as telling an undercover agent that he was irritated by several of the outcall services that compete with Mr. DeCarlo, and that "a couple of aspirins will be sent to Las Vegas to deal with those headaches." Mr. Congiusti's mob name is Vinnie Aspirins.

The indictment also quotes Mr. Stefano as stating that on one occasion Mr. Congiusti used a cordless drill to bore holes in the head of a man who had crossed the mob. According to the indictment, the F.B.I. agents who arrested Mr. Congiusti found a power drill in t he Ford Expedition he was traveling in at the time of the arrest.

The other alleged enforcer, Mr. Nelsen, is described in the indictment as a former mercenary soldier who is an expert in explosives. F.B.I. agents said that they has observed Mr. Nelson buying carburetor cleaner in an

automotive parts store and they believed he intended to use it to build a fire bomb.

Last Year, Hilda Brauer, an owner of the Perfect Body's and the Young and Sexy Bodies nude-dancing services, sued the Sprint Corporation and R.H. Donnelly co., publisher of the Las Vegas Yellow Pages, charging that they had conspired to divert telephone calls from her business.

Although the suit was dismissed, the accusations appear to have drawn the attention of Federal agencies. Several adult services operators who spoke on the condition of anonymity said that in the last year Federal agents had created an interagency computer crimes task force based in Reno to investigate call diversion. One of the service operators said he believed that call diversion had spread beyond the adult entertainment business and were becoming a growing problem for other Las Vegas businesses.

Federal officials in Las Vegas said they were familiar with the reports of electronic call diversion but for the time being were focusing on other charges, including suspected payoffs to local law enforcement officials.

"This is super big business here," Eric Johnson, an assistant United States attorney, said of sex services. "These operators generate a lot of money and a lot of cash."

The indictment charges that a significant portion of the Las Vegas out-call industry is a front for money laundering, robbery, narcotics distribution and other criminal activities, in addition to prostitution.

Federal agents believe that the mob is trying to grab control of the sex industry through illegal means, including sophisticated rerouting of calls from competitors' businesses.

The defendants face charges of conspiracy, extortion and interstate travel in aid of racketeering.

U.S. Department of Justice
United States Attorney's Office
Northern District of Texas
110 Commerce St., 3rd Fl.
Dallas, TX 75242-1699
Office: (214) 659-8600
Fax: (241)767-2898

For Immediate Release
Dallas, Texas
CONTACT: (214) 659-8707
September 16, 1999

United States Attorney Paul E. Coggins announced today that Corey Lindsly and Calvin Cantrell were sentenced today in federal court by the Honorable Chief District Judge Jerry Buchmeyer for hacking into computer systems belonging Sprint Corporation, Southwestern Bell and GTE, illegally obtaining long distance calling card numbers and selling these stolen calling card numbers.

Corey Lindsly, age 32, of Portland, Oregon, was sentenced to forty-one months imprisonment and ordered to pay $10,000 to the victim corporations. Calvin Cantrell, age 30, of Grand Prairie, Texas, was to two years imprisonment and ordered to pay $10,000 to the victim corporations. Both defendants pled guilty in late spring to Informations charging criminal fraud and related activity in connection with Access Devices and Computers, in violation of Title 18, united States Code, Sections 1029 (a)(3) and 1030(a)(4).

Lindsly and Cantrell are the major ringleaders in a computer hacker organization known as they "Phone Masters," whose ultimate goal was to own the telecommunications infrastructure from coast-to-coast. In addition to the numerous telecommunications systems that were penetrated, the group also penetrated computer systems owned by credit reporting agencies, utility providers, and systems owned by state and federal

governmental agencies, to include the Nation Crime Information Center (NCIC) computer. These hackers organized their assaults on the computers through teleconferencing and utilized encryption program PGP to hide the data which they traded with each other.

United States Attorney Coggins acknowledged the courage of Sprint Corporation, Southwestern Bell Corporation and GTE for coming forward to report this hacking into their computer system to the Federal Bureau of Investigation. United States Attorney…

http://www.usdoj.gov/criminal/cybercrime/phonmast.htm
11/26/01

Dallas/Fort Worth
WFAA.COM
wfaa>news>local

NEWS 8 INVESTIGATES
Cyber Terrorists Invade Phone Networks
By Robert Riggs
April 29 1999

http://people.ne.mediaone.net/kiad/hacker/
11/29/01

(photo)
GTE's network operations center at DFW International Airport was targeted by computer hackers.

DALLAS- It was the largest cyber-assault on the nation's communications networks.

A computer security breach received little attention when it was announced in Dallas last month. Hackers had been caught stealing thousands of long distance calling card numbers.

News 8 Investigates learned it was a case with national security implications.

A group of computer hackers invaded telephone systems so deeply that they could shut down 911 operators. In fact, they retaliated for a speeding ticket by crashing the phone system at a police department.

They also tipped off drug dealers to wire-taps.

Until now, this cyber-attack has been a closely-guarded secret. Computer hackers have broken into the networks of the world's largest telephone companies.

They were just a few keystrokes away from blinding air traffic controllers, shutting down banks, or cutting off military bases. It's not the plot of the latest cyber-horror movie.

This frightening penetration of the nation's telecommunications systems actually happened right here in North Texas.

The hackers' target list included GTE's 28-state network, controlled from a nerve center at DFW International Airport. They had the capability of causing a "cyber Pearl Harbor" had they wanted to.

FBI agents Mike Morris led the investigation. "We had a number of telephone companies, long distance carrier and local exchange carriers that thought they were impenetrable," Morris said. "They thought they were little castles."

HACKING HISTORY

The first confirmed break-in occurred four years ago when the hackers first took control of computerized phone switches. The switches route calls around the world. The hackers gained unrestricted access to GTE, Sprint, MCI and the regional Baby Bell networks.

Their early attacks went undetected, and alarmed top levels of the U.S. government. Details about the case are only now becoming public.

"They could listen in on calls made through that switch," Morris explained. "If they didn't like a person, they could turn their access off to that switch, meaning if you tried to make a call out, it wasn't going to happen."

FBI LAUNCHES CYBER SQUAD

A tip set in motion an intensive FBI investigation that continues today. In Dallas, a new cyber squad put a wiretap on the hackers' line. It marked the first time that agents could monitor everything a hacker typed.

"The goal of the hackers was to basically take control of telecommunications systems coast-to-coast," Morris said.

They came close.

THE PHONE MASTERS
FBI surveillance photos show some of the 11 hackers called the Phone Masters.

They gathered from across the country with cyber burglary tools in hand: a cloned cellular phone and laptop computer.

The FBI identified Calvin Cantrell of Grand Prairie as a central figure in the organization.

The hackers fit the FBI's profile:
-White Males
-Teens to mid-20's
-Self-taught
-Obsessed

"He wasn't very good at school, didn't make a lot of friends," Morris said of the individuals who fit the profile. "But when he gets on the Internet and he hacks into a system, now he basically is a cyber-God."

Even though the typical hacker is not a particularly good student, they are still brilliant. "Some of these guys could be considered geniuses," Morris said. 'they're very smart, and they get very bored with school."

The FBI discovered that Cantrell was an unemployed 1988 graduate of Grand Prairie High School. At his parents home, Cantrell spent up to 20 hours a day hacking into computer systems. The FBI said Cantrell took confidential credit and crime records out of computer systems and traded people's secrets for cash.

"Calvin represented himself as an information broker," said private investigator Trace Carpenter, who purchased personal information from Cantrell. He said Cantrell bragged about even getting phone records close to the President. "He was obtaining long distance records for Bill Clinton's mother," Carpenter said. "I suppose this was an effort to find a back line into the Oval Office, so to speak."

HACKERS TARGET WHITE HOUSE

Indeed, the Phone Masters hacked into White House phone records and unlisted numbers, according to sources in the telecommunications industry. "it shows the vulnerability of our everyday systems that we use," said Assistant.

Yarborough is now prosecuting the Phone Masters for stealing millions of dollars worth of long distance calling card numbers.

"Knowing and holding the keys to that system, any foreign agent or domestic hacker could choose to hack it," Yarborough is now prosecuting the Phone Masters for stealing millions of dollars worth of long distance calling card numbers.

"Knowing and holding the keys to that system, any foreign agent or domestic hacker could chose to hack it," Yarborough said. "That could have a wide-ranging impact on our financial institutions, power and electrical, the systems we use and interact with every day."

The FBI said the Phone Masters discussed crashing vital computer systems. It's unclear what the hackers may have done before the FBI got on their trail.

The hackers declined to talk to News 8.

Large-scale phone invasion goes unnoticed by all but FBI

December 14,1999
Web posted at: 3:39 p.m. EST (2039 GMT)
CNN.com

http://www.cnn.com/1999/TECH/computing/12/14/phone.hacking/ 1/9/02

In this story:

Calling card numbers, credit reports, and more
Giving the FBI the "pager treatment"
FBI agents turn the tables
Not as sexy, but more dangerous
Phonemasters' skills gave them a 'power trip'
Larger hacks slip under radar
RELATED STORIES, SITES

By D. Ian Hopper, CNN Interactive Technology Editor and Richard Stenger, CNN Interactive Writer

(CNN)- Where have all the hackers gone?
That's an understandable question considering the actions that currently pass for a news-making "hack." One might think that the days of Kevin Mitnick's phone hijinks or Robert Morris's computer worm, which disrupted the operations of over 6,000 computers nationwide in 1988, are gone.

Sure, there's malignant code like the Melissa virus which struck computers earlier this year, but so many viruses rely on users to knowingly or unknowingly pass them on until they finally strike. When they do strike, they usually just wipe out the user's hard drive – not so horrible, on a global scale.

But how about stories of intelligent hackers who download calling card numbers straight out of the data

banks of giant phone companies in order to use or resell them, download and resell credit reports or have the ability to reroute or even take down entire telephone networks at will? Those guys are gone, right?
Not so fast, They're far from done; they've just gone out of fashion.

Calling cards numbers, credit reports, and more.

A group of hackers called the Phonemasters, for example, stole tens of thousands of phone card numbers, found and called private White House telephone lines and rooted around in high-security FBI computer files in the mid-1990's.

But the gang behind ones of the largest hacks ever failed to see their names on one FBI list, a request to tap their lines. Some four years after U.S. agents busted the group, the last of three ringleaders now awaits sentencing in federal court.

Jonathon Bosanac pleaded guilty to two counts of computer-related fraud in a U. S. Court in San Diego last week. The self-proclaimed "Gatsby" faces sentencing on March 2.

Two other reputed ringleaders were sentenced in September. Corey "Tabbas" Lindsley received a prison term of 41 months; Calvin "Zibby" Centrell was given 24 months.

The hacker gang downloaded thousands of calling cards from AT&T, Sprint, and MCI to sell on the black market, according to federal prosecutors. Some of the reported retail customers included the Sicilian Mafia.

"One of the most valuable skills is to be a phone phreaker. If you 'own' the phone system, you have the keys to the kingdom; you can listen to anyone you want to, call forward, switch numbers and route calls," said Matthew

Yarbrough, the assistant U.S. attorney in Dallas who served as lead prosecutor in the case.

The scope of their activities was astounding. They could listen in on phone calls, alter secure databases and penetrate computer systems of credit reporting company Equifax and the FBI's National Crime Information Center.

Giving the FBI the "pager treatment"

The ringleaders even contemplated downloading every calling card in the United States, according to prosecutors.

A federal judge estimated that the group caused $1.85 million in business losses over three months.

The Phonemasters reportedly performed high-tech pranks, forwarding an FBI phone number to a sex chat line that left the bureau with a $200,000 tab. Some victims -- including a Pennsylvania police department that gave one Phonemaster a ticket—received the "pager treatment," in which their phone numbers were each sent to thousands of pagers.

The Phonemasters, a name coined by authorities, even sold for hundreds of dollars copies of personals credit reports, state motor-vehicle records and addresses or phone numbers of celebrities like Madonna and Danny Bonaduce.

"The information, because of the confidential nature, had a lot of value," Yarbrough said.

Looking through confidential databases, they warned targets of FBI surveillance that their phones were being tapped. But they never checked to see if their own phones were under surveillance.

The Phonemasters went to great measures to avoid detection during their long-distance conference calls,

never using their real names and speaking in code, referring to the calling card numbers as "tortillas," procecuters said.

FBI agents turn the tables

But they were often aware of the risk. In the transcript of one 1995 conversation, Bosanac hears a strange noise on the line.

"What the hell happened?" he asked.
"That was the FBI tapping in," Cantrell joked.
"You know how ironic that's going to be when they those tapes in court?" Lindsley said.

The FBI was listening, using a unique $70,000 prototype device that recorded every word and keystroke that moved along the phone line in Cantrell's home in Grand Prairie, Texas.

It marked the first time the FBI successfully eavesdropped on computer data traveling through telephone lines, federal prosecutors said.
In February 1995 a hacker friend told Cantrell his number was on a database of phone numbers under FBI watch. Soon FBI agents raided Cantrell's home, Lindsley's dorm room at the University of Pennsylvania in Philadelphia, and Bosanac's bedroom in his parents' house in Rancho Santa Fe, California.

It took more than four years before the three pleaded guilty to counts related to theft and possession of unauthorized calling-card numbers and unauthorized access to computer systems.

Lindsley who received one of the longest prison sentences in hacking history, refused to identify the voices of other hackers on tape.

Bosanac faces a maximum sentence of 15 years. His attorney Peter Hughes said that Bosanac will likely receive around 20 months in prison, in part because of his plea.

After the 1995 raid, Bosanac worked for a San Diego Internet company owned by AT&T, a Phonemaster victim. The company fired him after learning he had hacked into their system, a federal prosecutor said.

Bosanac, who remains free on a $25,000 bond, now works for a San Francisco firm that is aware of his case, Hughes said.

Not as sexy, but more dangerous

It's understandable if you haven't heard of the Phonemasters. With the exception of local newspapers reporting on hometown criminals or the so-called hacker media reports, the national media has largely ignored the Phonemaster and others like them.

"Lately the media has been caught up in Web defacement," said Yarbrough, who also leads the FBI's cyber crimes task force in Dallas.

The actions of Web defacers are typically confined to replacing the "home pages," or index files of a Web site with text and images that either- in the case of "hacktivism" – reflect a political or social viewpoint, or simply boast that the hacker had access to the site. Frequently, in an attempt to show no actual malice toward the site administrators, the hacker saves a copy of the original home page on the server or even leaves a text file containing a blueprint of how the hacker got access.

In its most common form, Web site defacement causes very little actual damage when compared to a large-scale intrusion like the ones made by the Phonemasters. But the site that has "I own you" scrawled on it is a lot more

obvious and brash than illegal charges made on thousands of calling cards. Hence, the graffiti artist gets what many of them want most: publicity.

That's not only a shame, say some computer crime observers, but its also very dangerous.

"The web graffiti kids really affect public perception," says Brian Martin, administrator of the Attrition.org site, which logs and comments on computer hacks. "Because of vague wording and unfounded comments, journalists often imply that because a Web page was defaced, an entire network was compromised. That is hardly the truth. Most of the time these kids couldn't touch the internal network.

Phonemasters' skills gave them a 'power trip'

To Martin, the public should be more worried about people with the skills of the Phonemasters.

"The level of knowledge they possess about computer systems, phone systems in particular, is amazing. In many cases they know more than highly paid and specialized technical operators of the systems they are into."

Martin suggests the Phonemasters were driven by two quests common to hackers: "learning and exploration." Then the just as common third purpose, a power trip. "They liked having access to any and all kinds of information."

Martin has written several essays urging "script-kiddies," a demeaning term for hackers who use ready-made programs written by others for braking into systems, to cease defacing Web sites. He writes that it's not worth the almost inevitable discovery and punishment by authorities for such little accomplishment as inconveniencing a site administrator for a few hours and scaring some customers.

"It disgusts me to see media attention being given to kids with scripts," Martin says. "Their annoying kiddie messages are a waste of time for all involved. Their weak justifications for hacking are only there to make them feel better about their activities and give it some sense of righteousness. The media dutifully inflates their egos when they get lucky and find some big corporate or military server vulnerable to the latest script they got."

Larger hacks slip under radar

Space Rouge is an employee of Boston-based L0pht Heavy Industries, a hacker think tank, and is the editor of Hacker New Network. He suggests that the Phonemasters have slipped under the national media radar because their intrusions are phone-based, and don't specifically involve the Internet.

"The Internet is the hot technology topic at the moment and has been for some time. If it does not involve the Internet, people don't want to report on it. But this is a major crime and should be reported on. I just don't understand it," he says.

Like Martin, Space Rogue thinks the skills of the Phonemasters go far beyond the abilities of the Web graffiti artists.

"The phonemasters can not be compared to script-kiddies in anyway. The first are knowledgeable people who have learned systems inside and out. Script-kiddies can click a mouse button that says 'run'. There is absolutely no comparison."

Those "script-kiddies" shouldn't feel like their acts are being ignored by authorities, though. As the Internet continues being a vehicle for commerce, Web site defacements are increasingly having economic consequences.

Attacks against electronic business and government sites "both carry big problems. It's not the equivalent anymore to spray painting billboards on the highway," U.S. Attorney Yarbrough warns.

If e-commerce sites have to be closed to repair defacements, those companies can lost tens of millions a day in lost revenue, he said.

Martin, who mentions that the Phonemasters taught him some tricks as well, praises the Phonemasters for their restraint.

"They had the power to destroy entire companies, crash phone networks and more. Yet they didn't."

"The real evil is guys with the Phonemasters' skill set, but a lot less ethics," Martin says.

LV man, son held in computer scam

By: John Glisch
Review Journal

A Las Vegas man and his 16-year-old son were arrested at their home Friday and charged with *** Nevada Central Telephone of at least $50,000 by using a computer in the son's bedroom to make long-distance phone calls.

Central Telephone officials also said the pair plugged into other computer systems nationwide, including one of a major fast-food chain with the aid of what they called fellow "telephone freaks" in different parts of the country.

Metropolitan Police said Edward Kantor, 38, 4466 Avondale, was charged with avoiding payment and possession of an instrument. He remains in custody at the Clark County Jail under $51,000 bond.

The youth, a student at Chaparral High School, was placed under the custody of juvenile authorities.

Authorities said the arrests occurred about 4 p.m. following a six-month investigation by Central Telephone, in which security technicians used highly sophisticated surveillance equipment to monitor telephone calls from the house.

Sal Cinquegrani, a public information official with Central Telephone, said the pair had apparently been utilizing the computer scam for at least a year making a still undetermined number of calls.

"They made 40 calls on Thursday alone," he said.

Cinquegrani said the investigation began after routine checks showed a large number of long-distance calls were made and placed on monthly bills of other people.

He said by using a home Apple II computer, the pair was able to plug into telephone lines and by-pass Central Telephone's computerized billing system.

"Once they did that, they were talking to other computers," he said. "It's a nationwide scam. What it boils

down to is that you and me were paying for all those services."

Besides entering Central telephone's computers, Cinquegrani said the pair hooked into the computers of other "telephone freaks" across the country, getting the codes for "multiple" business computer systems locally and nationwide.

Cinquegrani said apparently as a prank, the pair entered the system of a major fast-food chain where they changed records to show increased overtime along with adding employees to the payroll.

"They can do all sorts of things and it's havoc." He said.

Cinquegrani also said the surveillance uncovered others in the Las Vegas area apparently using the same computer scam methods.

"There are several other phone freaks that were introduced to us through this investigation," he said, "We know who they are and we will prosecute them."

Cinquegrani went on to say a large amount of homemade electronic equipment, as well as telephones and computers, was confiscated from the Kantor home.

It was also learned Kantor is an employee of Telephone World, 1431 Charleston Ave., an independent seller of telephone equipment.

FBI boss moving up
Friday, December 18, 1998
Las Vegas Review Journal

Bobby Siller, the special agent in charge of the Las Vegas office of the FBI, is retiring from the bureau and will become a member of the state Gaming Control Board.

Siller has led one of the most active bureau offices in the history of the city. He also has made no secret of his desire to remain in the community. Recent FBI cases include several investigations into organized crime presence on the streets of Las Vegas. Among those investigations: the murder of Herbie Blitzstein and the alleged hostile takeover attempt of the local out call entertainment racket.

Siller's agents also are largely responsible for putting together a devastating case against slot cheating kingpin Dennis Nikrash, who is now cooperating with the government.

But not even Siller could fix the phone system at the local FBI office, where agents earlier this week were complaining that the leading law enforcement agency in the nation needed a bank of pay phones.

Although the bureau does not often promote from within for the special agent in charge position, Siller's assistant, Walt Stowe, has the kind of credentials that make him the painfully obvious choice for the job.

Stowe is a 26-year agent with six years in administration in Las Vegas, which even by FBI standards is unique among major cities.

If Stowe can do something with that phone system, I say he deserves the job....

State takes on high-tech crime

A new pamphlet offers tips to help businesses reduce the chances of becoming criminal victims.

By Sean Whaley
Donrey Capital Bureau

CARSON CITY – A task force formed to help businesses fight high-tech crime has prepared a pamphlet with tip to reduce the risk of theft, embezzlement and fraud.

Among the suggestions from the attorney general's office and the High Technology Crime Task Force anyways to avoid having long-distance phone calls improperly charged to business accounts and how to secure confidential client and customer information.

"The cost of high technology crime to business is staggering and expected to increase dramatically by the end of the decade," she said.

According to FBI statistics, computer crime costs American businesses between $5 billion and $10 billion annually. By the year 2000, that figure could increase to as much as $200 billion, Del Papa said.

The goal of the state's task force is to assess what resources are needed to help give law enforcement agencies the ability to better investigate and prosecute high-tech criminals. Business involvement is essential, and Del Papa asks people with expertise or equipment to contact her office at 486-3420 in Las Vegas. A copy o the pamphlet also can be obtained at this number.

The brochure, entitled "Tips for Businesses to Fight High Tech Crime," contains a variety of suggestions, including training employees to check credit card numbers and to compare information on the face of a credit card with the information printed out on the receipt.

Other tips include changing pass-words and locks when an employee quits or is fired, and keeping banking or other confidential data on a different computer than ones used for Internet services.

STRIP ADVERTISING
P.O. BOX 61344
LAS VEGAS, NV 89160

I hand delivered Phone Records of M.G.C. and Telco to the FBI Special Agent Dave Van Zant.

Date
December 8, 1998

(s)_____
Eddie Munoz

Received By:
(s)_____

STRIP ADVERTISING
P.O. BOX 61344
LAS VEGAS, NV 89160

I hand delivered Phone Records of M.G.C. and Telco to the FBI Special Agent Dave Van Zant.

Date
December 16, 1998

(s)_____
Eddie Munoz

Received By:
(s)_____

(Notes of Eddie Munoz in relation to the FBI investigation that has gone on for a number of years before taking this problem to the PUC of Nevada)

9-7-99 @ 1:00
Federal Bureau of Investigation
Las Vegas
ESCORTED

FBI Building
Jerry Hanford – Strike Force
Ray Le Ber – Agent Computers

{call back this week}

9-27-99 Tuesday @ 1:00
Federal Bureau of Investigation
Las Vegas
ESCORTED

Jerry Hanford
Eric Johnson
2 hr meeting

8-25-99 @ 10:00
Federal Bureau of Investigation
Las Vegas
ESCORTED

My grandfather- Retired Judge Abraham Bowling
attended with me.

Jerry Hanford
Special Agent
Federal Bureau of Investigation
636-5063
702-385-1281
2005 Charleston Blvd.
Las Vegas Nevada 89104

AFFIDAVIT OF EDDIE PAUL MUNOZ

I, EDDIE PAUL MUNOZ, being first duly sworn under oath hereby swear that the information set forth herein is true and correct to best of my knowledge.
SWORN TO UNDER PENALTY OF PERJURY;
THAT, I, Eddie Paul Munoz, own and operate a licensed business by the name Las Vegas Informer in the Las Vegas area; where I have signed into Contracts with the Telephone Company doing business as Sprint.
THAT, all the information in support of my claims of Sprints phone lines causing my business to operate with un-secure phone lines are true and correct to the best of my knowledge.
THAT, until my phone lines having become un-secure the Las Vegas Informer was operating as a profitable business and not losing money like it has been as a result of my phone lines being compromised.

Respectfully Submitted:
(s)_____
Eddie Paul Munoz, Pro Se

DATED; on this _____ day of
----------, 2004

NEVADA INVESTIGATIVE SERVICES
P.O. Box 91434
Henderson, NV 89009-1434
(702) 566-8008

October 16, 1998

Jerry B. Holmes
Consumer Services Representative
State of Nevada
Public Utilities Commission
Consumer Division
555 E. Washington Avenue No. 4500
Las Vegas, NV 89101

Confidential
Privileged
Communication
NRS.41.550

Re: Born vs. Sprint of Nevada
File: CCU-092298-JB

Dear Sir:

Thank You for your acknowledgement and action taken, regarding my September 9, 1998 complaint.

On October 14, 1998, the United States Attorney's Office, filed in U.S. District Court, the attached "Complaint", sworn to by Charles Maurer, Special Agent of the Federal Bureau of Investigation. This complaint, in part, is associated with my investigation regarding the Hilda Brauer case, eluded to in my original complaint to your office and does stand to help prove that my allegations of telephone diversion may have in fact taken place. Investigator Ron Heilman, of my office, in accompany with Hilda Brauer, were the first persons to bring the matter of telephone diversions to the attention of the FBI. Said investigation identified Richard Soranno (mentioned in the attached report), as a possible responsible.

While the attached complaint identifies other person(s) found in the Brauer investigation, it also details to the reader, what if their intent was in diverting calls. I offer to you testimonial evidence, before the court, that

such telephone diversion may have in fact taken place, as follows: with reference to page (5) of said report, which reads in part "... such as the use of electronic means to divert calls from competitors businesses...".With reference to page (11), "...Charles Coveney. Pugliese said that Coveney is a computer expert who currently works for Soranno. Coveney has contacts in the Sprint Telephone Company and is able to have telephone calls diverted from one number to another."

It would appear that the FBI has taken a significant step in identifying those responsible at the Sprint Telephone Company, for possibly diverting my telephone and causing my business to suffer financial disaster. Although the exact name(s) of the mentioned telephone company employee(s) are still undisclosed, I would suspect that they are known to the FBI and that disclosure is forthcoming.

In fairness, I think I should receive a letter of apology and be compensated by the telephone company for any disclosed criminal actions by their employee(s). I am very concerned about the possibility of telephone interception through eavesdropping. Certainly anyone empowered with the knowledge, opportunity and ability to divert a line, may also be able to listen in on my conversations with my investigator or client in the Brauer case. To that end, I am becoming concerned with the possibility that client-investigator confidentiality laws, may have been violated, through this alleged breach of public trust. As an investigator, I routinely receive private and confidential information over the telephone, from attorneys and other persons of all positions and walks of life. I am unclear as to what extent your office can do towards bringing about customer satisfaction in my complaint. One thing is for certain and that is, in my opinion, I cannot trust the Sprint Telephone Company and absent any immediate remedy, may find it necessary to address my grievance in U.S. District Court.

If the aforementioned federal intervention (FBI) into your investigation, into this very same matter, stands on its merits to conclude your investigation, I would

request that you so advise the Sprint Telephone Company and make any recommendations at that time, for possible settlement options. Again thank you for your help in this matter, I look forward to hearing from you soon.'

Respectfully Submitted,
(s)_____
James T. Born

STATE OF NEVADA
PUBLIC UTILITIES COMMISSION OF NEVADA
727 Fairview Drive
Carson City, Nevada 89701-5451
Policy (702) 687-6007 – Fax (702) 687-6110
Staff (702) 687-6001 – Fax (702) 687-6120

FAX TRANSMITTAL

DATE: 10/20/98
TO: Kathy Hodge
FROM: Jerry Holmes
21 PAGE(S) INCLUDING THIS COVER LETTER. IF YOU HAVE ANY QUESTIONS, PLEASE DO NOT HESITATE TO CALL ME AT (702) 486-2600 OR FAX TO (702) 486-2595.

Addition to Complaint CC4-092298-JB
Please Respond to the compensation claim in the cover letter from Mr. Born on page 2, paragraph 2, line 1.

CONFIDENTIALITY NOTICE: The document(s) accompanying this telecopy transmission contains confidential information belonging to the sender which is legally privileged. The information is intended only for the use of the individual or entity named above. If you are not the intended recipient, you are hereby notified that nay disclosure, copying, distribution, or the taking of any action in reliance on the contents of this telecopied information is strictly prohibited. If you have received this telecopy in error, please immediately notify us by telephone to arrange for return of the documents to us.

KATHRYN E. LANDRETH
United States Attorney
KURT P. SHULKE
Attorney in Charge
ERIC JOHNSON
Assistant United States Attorney
Organized Crime Strike Force
United States Attorney's Office
701 East Bridger Avenue, Suite 550
Las Vegas, Nevada 89101
702-388-6363

FILED
JUL 13 1999
CLERK U.S. DISTRICT COURT
DISTRICT OF NEVADA
BY (s)_____DEPUTY

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

-o0o-

UNITED STATES OF AMERICA,

Plaintiff,

v.

CHRISTIANO DeCARLO, also known as Chris DeCarlo,
MARIO STEFANO, also known as Mario Pugliese,
ANTON NELSEN, KENNETH BYRNES, and
JOSHUA SNELLINGS, also known as Josh Snellings,

Defendants.

CR-S-98-375 (PMP)(RLH)

INDICTMENT for violation of Title 18, United States Code, Sections 1951, Interference with Commerce by Threat of Violence (Hobbs Act); 1952, Interstate Travel in Aid of Racketeering Activity; 924 (c) Possession of

Firearm During a Crime of Violence; 371, Conspiracy; and 2, Aiding and Abetting

---

THE GRAND JURY CHARGES THAT:

COUNT ONE
(Interference with commerce by threats or Violence with Aiding and Abetting)

1. At all or part of the time material to this Indictment, Frank Bartello, Richard Soranno and Harry Jacobs directly or indirectly owned and operated out call services in the Las Vegas, Nevada, area for the purpose of providing female and male entertainers to individuals in exchange for money, which businesses affected interstate commerce.

2. At all or part of the time material to this Indictment, defendant CHRISTIANO DeCARLO directly or indirectly owned and operated an out call service in the Las Vegas, Nevada, area for the purpose of providing female and male entertainers to individuals in exchange for money, which business affected interstate commerce. Defendant CHRISTIANO DeCARLO's out call service competed for customers with Frank Bartello's, Richard Soranno's and Harry Jacobs' out call services in the Las Vegas, Nevada area.

3. At all or part of the time material to this Indictment, defendants perceived Charles Coveney as an individual who worked for one or more out call businesses in the Las Vegas, Nevada, area and who, through use of computers and computer networks, was capable of controlling the Sprint telephone system in southern Nevada, which telephone system affected interstate commerce, to divert telephone calls from defendant CHRISTIANO DeCARLO'S and other individuals' out call services to Richard Soranno's and possibly other competitor's out call services for the purpose of diverting customers from defendant CHRISTIANO DeCARLO's and other individuals' out

call services to Richard Soranno's and possibly other competitor's out call services.

4. From on or about June 1998, through and including the date of this Indictment, in the District of Nevada and elsewhere,

CHRISTIANO DeCARLO, also known as Chris DeCarlo,
MARIO STEFANO, also known as Mario Pugliese,
ANTON NELSEN, KENNETH BYRNES, and
JOSHUA SNELLINGS, also known as Josh Snellings,...

(page 11)

...were arriving on October 7, 1998, and intended to meet with and possibly make an example of the previously described owners of out call services.

22. On October 5, 1998. UCA and CW-1 met Pugliese in New York City. CW-1 was wearing a hidden body recorder during this meeting. Pugliese advised he is sending two individuals from Tampa, FL to Las Vegas, Nevada, to assist Byrnes in dealing with Bartello, Soranno and Jacobs, all of whom are out call service operators. Pugliese advised one of the individual coming to Las Vegas is known as "Vinnie Aspirins" and the other is a former mercenary. Pugliese said that Vinnie 'Aspirins' has a reputation for torturing people. Pugliese advised on one occasion Vinnie 'Aspirins' used a cordless drill to drill holes into an individual's head.

23. On or about October 5, 1998, Pugliese told CW-1 that in addition to the out call business operators targeted, he has targeted an individual named Charles Coveney. Pugliese said that Coveney is a computer expert who currently works for Soranno. Coveney has contacts in the Sprint Telephone Company and is able to have telephone calls diverted from one number to another. Pugliese expects to persuade Coveney to leave Soranno and assist DeCarlo in his out call business by diverting telephone calls to DeCarlo.

24. On or about October 5, 1998, during a meeting between CW-1, UCA and Pugliese, Pugliese

advised that he was involved in a cigarette smuggling operation in the Bahamas. In an attempt to raise money for this smuggling operation, Pugliese and his associates from Tampa Florida, met with an unnamed individual and "persuaded" his against his will to sign over a $300,000 lien on a ...

NEVADA INVESTIGATIVE SERVICES
CRIMINAL- CIVIL- DOMESTIC
EXPERIENCE SINCE 1969

JAMES T. BORN – Private Investigator

Main office:
P.O. Box 91434
Henderson, Nevada
89009-1434
(702) 564-4357
(702) 566-8008

STATE LICENSE:
Nevada 457
California AQ007195
Nevada 56

CONTRACT

The undersigned hereby hires NEVADA INVESTIGATIVE SERVICES, its agents and employees to perform the following confidential investigative service(s):

Attempt to conduct a telephone sweep to determine if a phone tap is in place on the business lines. Attempt to assit client to determine if she is the victim of industrial sabotage. Client grants permission for NIS to tape record certain telephone conversations on her business lines. Between NIS and her business x_____
For the purpose of this contract client is acting in proper person.

The undersigned hereby agrees to compensate NEVADA INVESTIGATIVE SERVICES for any and all work commenced through verbal agreement, prior to the execution of this contract. The undersigned- understands and agrees that all work begins upon verbal or written receipt of the clients order. Subject investigation will

commence on 10-27-95 and continue until completion of said service, or receipt of written notice of termination by the undersigned.

The undersigned hereby agrees to compensate NEVADA INVESTIGATIVE SERVICES for the performance of said services as follows:

$350.00 for phone sweep
$450.00 for in house phone calls

$800 plus hotel room rents

If case goes to lawsuit, NIS will receive 10% of award for work.

The undersigned agrees to pay all monies doe on the date said charges and expenses are invoiced. The undersigned agrees to pay for any and all court, or other fees that may be necessary to collect unpaid monies.

NEVADA INVESTIGATIVE SERVICES agrees that its agents and employees shall use reasonable diligence and due care in performing the above described investigative service(s), and that said services shall be performed in conformity with all applicable laws, ordinances, and regulations pertaining to Private Investigators, NEVADA INVESTIGATIVE SERVICES, however, does not, nor can it, warrant that its agents and employees will successfully achieve the anticipated results of the above described investigative services. Accordingly, the undersigned, being fully cognizant of the risks and uncertainties involved in performing said services, agrees to compensate NEVADA INVESTIGATIVE SERVICES for services performed on his or her behalf, as set forth above, regardless of outcome.

The undersigned further acknowledges that NEVADA INVESTIGATIVE SERVICES, its agents and employees, are being hired to perform investigative services only, and have no personal stake in the results of

their effort, or the use of those results by the undersigned. Accordingly, the undersigned agrees that NEVADA INVESTIGATIVE SERVICES shall be in no manner responsible for the use of these results, and hereby agrees to hold NEVADA INVESTIGATIVE SERVICES , its agents and employees, harmless from any and all cost, loss, expense, claim, or liability which may arise from the use of said results.

In the event that legal action is commenced in order to recover the compensation referenced above, NEVADA INVESTIGATIVE SERVICES , in addition to any other remedy in law or equity to which it may be entitled, shall in addition to that already mentioned in this contract, shall be entitled to an award of all attorney's fees and costs incurred.

The undersigned agrees to pay any required retainer fee by the end of the third working day from the time the investigative services were requested, the undersigned further understands that NEVADA INVESTIGATIVE SERVICES may stop work and demand compensation for investigative expenses incurred, including time exhausted, for non payment. Undersigned is hereby informed that with reference to Chapter 648, Nevada Revised Statutes "Upon demand by the customer, the license shall not refuse to divulge to the customer the results of an investigation if payment has been tendered for charges levied."

DATE: 10-26-95
$500.00 Cash Paid 10-26-95
$300.00 Balance Due 10-31-95

(s)_____
Hilda Brauer
(NAME)
(Agency Representing)

(s)_____
JAMES T. BORN
Private Investigator

EXHIBIT 4E – DATA REQUEST

Diversion
Rio

The Rio Incident was a call diversion where a couple had called our number and received a company called "Room Service" that ripped the customer off. In the morning he was going to call metro and file a complaint. So I went and showed him our phone records of the night that show we did not receive his call. His wife wrote a statement of the incident and gave us a copy of their hotel bill which gave our telephone number as the only one dialed number. Later the investigation turn up that Room Service was Frank Bartello who dispatched the "Cody & Daphne" scenario- they identified girls from Room Service office. This incident was documented with the Organized Crime Detectives Roy Brotherson and Gayland Hammack. Rio video surveillance tapes were pulled to identify the girls.

MUNOZ' EVIDENCE OF CALL DIVERSION

Munoz contacted Scott Collins, Sprint Docket Manager, in January 2001 and said that he had obtained proof of call diversion. Munoz stated that a tourist staying at the Rio hotel called one of Munoz' toll free telephone numbers and ordered a female escort. The female escort arrived at the hotel room and asked the tourist what type of girl he wanted. The female escort offered to get whatever type of girl the tourist desired, but required a $125.00 deposit. The escort took the money and did not return to the hotel room. The tourist called Munoz the next day and demanded to know why the escort took the money and did not return. Munoz had no record of the tourist's initial call from the Rio hotel. Munoz offered the tourist a 125.00 if he could produce a receipt from the hotel reflecting that Munoz' toll free number was dialed from the room. The tourist produced a hotel bill with Munoz' toll free telephone number listed on the bill. Munoz also had the tourist signed and date a letter detailing his experience with the female escort. Munoz claims that he did not receive the call from the tourist at the Rio hotel. He stated the escort that went to the Rio was not affiliate with Munoz' service. Munoz confidently states this is proof that calls are being diverted from his business. Munoz claims that Sprint's network is being compromised internally or possibly by an outside entity such as a hacker.

As a result of Munoz' claim of call diversion from the Rio hotel, Scott Collins rented a room at the Rio on Friday, February 16, 2001 to place several test calls. Munoz was notified of the test calls from the Rio approximately four hours before the test started. Mr. Collins placed a total of forty test calls from the hotel room in the presence of Rich Stephenson, Sprint Western Regional Security Manager, and Barry Holt, Senior Consumer Investigator for the NPUC. Of the forty calls placed, six calls did not go through. Of the six calls that did not go through, only two toll free numbers were affected. Three attempts to reach one toll free telephone number terminated to a busy signal

and three attempts to reach the other toll free number terminated to an unknown pager. It is unknown at this point why the calls went to a pager. This will require further investigation.

CONCLUSION

In conclusion, Sprint has spent a tremendous amount of time and resources investigating Munoz' allegations. A total of 245 test calls have been conducted on Munoz' toll free telephone numbers from six different hotels. There has been no evidence of any call diversion or dropping of calls during any of the tests, Commission Soderberg ruled on February 22, 2001, that Munoz has provided enough circumstantial evidence to warrant a hearing. The Commissioner warned Munoz that he must provide substantial proof of where the call diversion is taking place, not just show evidence that he is not receiving calls.

(Letter from the customers staying at the Rio)

To Whom It May Concern:

On 1-5-01 we called to have a female entertainer come to our hotel room. A girl came and took $125 from us. She said she charged *** dollars. She said her agency would send a girl who charged just $125. The girl kept the $125 and said the next girl would be here in 15 minutes. However, The girl never came. Then we called the agency in the AM, They said they never got the call. The agency came to our hotel room on Saturday afternoon and gave us $125. My husband called the agency – got a copy of our phone bill that has the agency number on it. However, the agency shows no record of our call. The agency now has a copy of our bill as proof of this call.

(s)_____

Vickie L. Lacher

RIO SUITE HOTEL & CASINO
LAS VEGAS

I CONFIRM MY DEPARTURE DATE AS STATED. I ACKNOWLEDGE THAT A $50.00 FEE WILL APPLY IN THE EVENT THAT I DEPART PRIOR TO THAT DATE.

THOMAS OR
VICKEY L LACHER

Arrival: 1/03/01
Departure: 1/07/01
Persons: 2
Date: 1/03 $70 1/04 $70 1/05 $70 1/06 $70
Group Code: BDAIRY
Account# 367234416003
Room Type: IT K1EH
Room# 1125
Deposit Received: 76.30 FVS 4444000764003170

GUEST ROOM SAFES ARE PROVIDED. HOTEL ASSUMES NO RESPONSIBILITY FOR LOSS OF VALUABLES NOT DEPOSITED IN GUEST ROOM SAFES.
I AGREE THAT MY LIABILITY FOR THIS BILL IS NOT WAIVED AND AGREE TO BE HELD PERSONALLY LIABLE IN THE EVENT THAT THE INDICATED PERSON. COMPANY OR ASSOCIATION FAILS TO PAY FOR ANY PART OR THE FULL AMOUNT OF THESE CHARGES.

TE	DESCRIPTION	AMOUNT	BALANCE DUE
	ROOM CHARGE		
2001	1125	$70.00	$70.00
2001	TAX	$6.30	$76.30
	APPLIED		
2001	DEPOSIT	$76.30	$0.00
	ROOM CHARGE		
2001	1125	$70.00	$70.00
001	TAX	$6.30	$76.30

	LOCAL/PHONE					
)01	ACCESS	8987526	:12	16:55	$1.00	$77.30
	LONG DISTANCE					
)01	CALL	8888959808	:04	00:57	$1.00	$78.30
	LONG DISTANCE					
)01	CALL	8887082254	:08	01:18	$1.00	$79.30
	LOCAL/PHONE					
)01	ACCESS	8987526	:34	01:25	$1.00	$80.30
	ROOM CHARGE					
)01	1125				$70.00	$150.30
)01	TAX				$6.30	$156.60
	LONG DISTANCE			5:56		
)01	CALL	88873333066		08:37	$1.00	$157.60
	LOCAL/PHONE					
)01	ACCESS	7367544	:44	23:43	$1.00	$158.60
	LOCAL/PHONE					
)01	ACCESS	8987526	:10	10:29	$1.00	$159.60
	LONG DISTANCE					
)01	CALL	8887082254	:34	10:37	$1.00	$160.60
	LONG DISTANCE			7:42		
)01	CALL	8887082254		10:51	$1.00	$161.60
)01	ROOM SERVICE I				$25.11	$186.71
	LONG DISTANCE			3:06		
)01	CALL	8887082254		11:16	$1.00	$187.71
	BALANCE					$187.71

RIO

Flamingo at Valley View
(800) 888-1808 – (702) 852-7777
Post Office Box 14160 – Las Vegas Nevada 89114
Website www.playrio.com

RIO SUITE HOTEL & CASINO
LAS VEGAS

In Suite Phone Rates

- Local and Toll Free Calls: $1.25 per call (Please be advised that any toll free calls which exceed 20 minutes in length will be subject to a charge of $.25 per minute for each minute over 20. Any local calls which exceed 10 minutes in length will be subject to a charge of $10 per minute for each miute over 10.
- Long Distance Calls: $1.25 per call access fee; per minute rate is established at the AT&T Operator Assisted Day Rate + 65% hotel surcharge
- Collect, Operator Assisted and Credit Card Calls: $1.25 per call access fee + applicable provider surcharge
- Directory Assistance (Long Distance): $1.25 per call by dialing 9+1+Area Code+555-1212
- Alternate Long Distance Carriers: Please refer to the access information provided by your long distance carrier's calling card.

ALL CALLS ARE CONSISTANT WITH CURRENT LEGISLATION.

Address consumer complaints to:
FCC Consumer Protection Branch
CCB Mail Stop 1600A2
Washington, DC 20554
-Or-
Nevada PUC
1150 E. Williams
Carson City, NV 89701
(702) 687-6000

Reservations (800) 888-1808
(702) 252-7777 - Flamingo at Valley View
Post Office Box 14160, Las Vegas, Nevada 89114

Excerpt from
Direct Testimony of Scott B. Collins
October 23,2001
Eddie Munoz v. Central Telephone Company-Nevada
(Pages 34-41)

...service. But it wasn't anything formal. It was just more of a follow-up to make sure he was getting his calls.

Q: as a result of these less formal tests, as I'll call them, was there any indication that Mr. Munoz was not getting his calls?

A: I was never informed that Mr. Munoz was not receiving his calls. As far as i know, everything was working through Sprint's network fine. I have seen notes and trouble tickets that said X number of calls went through. But I was never informed that Mr. Munoz was not receiving his calls.

Q: Did you ever see notes and trouble tickets saying that not all the calls were going through?

A: I don't recall seeing anything – or any notes saying that the calls were not going through. I do recall seeing that, for example, say, 100 calls went through, and 95 were answered by the subscriber, which would be Mr. Munoz.

And those numbers, I've just made up.

Q: I understand.
What would that mean to you?

A: that would mean that the calls went through Sprint's network and went through to Mr. – or went through to the network interface device on the side of Mr. Munoz's house, but were not necessarily answered on Mr. Munoz's place of business.

Q: Using your hypothetical of 100 calls being made and 95 being answered, what would happen to the other five calls?

A: They may have just rang and were never picked up.

Q: Would that be the only explanation?

MR. REILLY: Objection. Calls for speculation.

THE WITNESS: That's what I would assume.

BY MR. ALPERT:

Q: Do you know a gentleman by the name of Joe Spears?

A: Yes.

Q: Who is Mr. Spears?

A: Mr. Spears is a security officer with corporate security for Sprint.

Q. Has Mr. Spears been involved in the investigation of the Munoz complaint?

A: He's been involved, but not really actively participating. He was with – he accompanied myself during the night of the tests in November in the hotel rooms and once when we went to visit Mr. Munoz.

Q: Was he with you on the first test in November?

A: Yes.

Q: I did not hear his name before.

A: Well, I believe when I gave those names. I said that were actively participating, Mr. Spears was just with me as a witness in the room. He didn't really have any active participation.

Q: Did you and Mr. Spears visit Mr. Munoz at his place of business in February of 2001?

A: I'm not sure of the date. But, yes. Mr. Spears and I did visit Mr. Munoz at his place of business.

Q: Would it have been sometime early in 2001?

A: Yes.

Q: What was the purpose of that visit?

A: I believe the purpose was to meet with Mr. Munoz and discuss the possible problem with the hotel bill at the Rio because Mr. Munoz called me up and said he had proof that he was having a problem with his service.

Q: The hotel bill is the one we just discussed, Exhibit 5?

A: Correct.

Q: So you had discussed that previously with Mr. Munoz?

A: Yes.

Q: So you and Mr. Spears came to see Mr. Munoz?

A: Yes.

Q: And what did you guys discuss?

A: Mr. Munoz showed me the hotel bill, which is Exhibit 5, and explained to me that a customer had contacted him and was upset, that he ordered an escort from Mr. Munoz, and that escort arrived and took some money and then left.

And then Mr. Munoz received this hotel bill from the customer. And Mr. Munoz pointed out to me that one of his telephone numbers were called from the Rio but that his records did not indicate that he received that call from the Rio on that date and that time.

Q: Did you investigate that complaint?

A: My investigation was renting a room at the hotel – or at the Rio Hotel and conducting test calls myself to see if I could replicate the same problem.

Q: So the February testing that we've already discussed was a result of you talking with Mr. Munoz about the Rio phone bill?

A: Yes.

Q: Were you ever able to determine from the Rio phone bill why the number went – why the call went to a different number?

MR. REILLY: Objection. Assumes facts.

THE WITNESS: No.

BY MR. ALPERT:

Q: Did you do anything to see if you could make such a determination?

A: The only thing I could do was place test calls from the Rio to see if the same problem happened again. But other than that, we don't own the hotel – Rio's P.B.X. switch, so I really couldn't do anything.

Q: Did you do anything to determine the identity of the phone numbers – the three numbers listed in Exhibit 6?

A: I've never seen those numbers before today. This is the first I've ever seen them or been made aware of these calls – or these numbers.

Q: Well, at least one of them shows up in Exhibit 7; is that correct?

A: Correct. But I don't believe I've ever seen a copy of Mr. Munoz's bill, as Exhibit 7. This is the first time I've ever seen it.

Q: Fair enough.
When you and Mr. Spears met with Mr. Munoz earlier in 2001, did you indicate to him that there was a problem was?

A: I was certainly perplexed as to why the customer at the Rio called Mr. Munoz's number, and, according to Mr. Munoz, he said that he never received the call.

Q: As a result of that meeting with Mr. Munoz, do you – did Sprint do any further testing on Mr. Munoz's lines?

A: Not a result of that, no.

Q: Was there further testing done on his lines early in 2001 for other reasons?

A: I believe it was just part of the continuation of monitoring the flow of traffic over at Mr. Munoz's facilities. And the monitoring of those calls were a result of Mr. Munoz's repeated effort of placing trouble tickets with Sprint saying he was having problems with his service.

So the testing was just a result of those trouble tickets and Mr. Munoz's allegations of service problems.

Q: Did Sprint ever determine that there was a bridge tap on any of Mr. Munoz's lines?

A: Yes.

Q: Tell me first what a bridge tap is.

A: Mr. Munoz has a T-1 service, which is a direct connection between Sprint's servicing central office, the East 7 Central Office to Mr. Munoz's business. And bridge tap is the unnecessary connection of other cables and pairs to the direct electrical path.

A T-1 cannot operate properly with any bridge tap on the line. So what the technicians did is—in investigating Mr. Munoz's claims, they determined that there was a bridge tap on there, which would possibly degrade Mr. Munoz's service

So they just simply removed the bridge tap, which is a normal procedure. It happens on a daily basis.

Q: How did the bridge tap get placed on the line?

MR. REILLY: Objection. Calls for speculation. If you know.

THE WITNESS: Well, I'd like to state that I'm not a technician. I've never received any type of formal training or anything like that.

But all a T-1 is a twisted pair of copper wire that runs from the East 7 Central Office to Mr. Munoz's business. That same twisted pair of copper wire can be used for plain old residential telephone service. And as that cable is distributed out into the network, it fees off to different areas.

In order to have a T-1 working properly, what the technicians do is they go out and they remove any excess feeding of that cable so it's just a direct electrical path or digital path to Mr. Munoz's residence. And it's not a complicated process to remove bridge taps.

BY MR. ALPERT:

Q: Is a bridge tap something that Sprint installs?

A: It's not necessarily installed. It's the way our outside plant facilities are distributed out into the field. The cable bridges off and sections out. And that's just the way our network is designed.

And when a T-1 service is requested by a customer, the technician installing should check for the bridge tap and remove it. Bridge tap is nothing that's added by Sprint. It's just the way our network is laid out and they way our facilities are...

(Notes taken by Eddie Munoz at the time of the "Rio Incident")

Steve
10-4-01

Van Nuys
818-933-8808
Number on a Sprint Bill
- - - - - - - - - - - - - - - - -
Dial From Rio Room
1-818-933-8806
1-818-424-3080
1-818-933-0023
State to State
- - - - - - - - - - - - - - - - - -
257-3255
11-11 818-933-8806 Travel Lodge 736-3443
Don – Motor Bill

314-4730 Sahara 737-2111
Vickie – Supervisor ID#
Espire- 474-710
Cindy
Espire Michelle does not know

Jim Harding does do know
VA- 1-800-937-7473

14th 4 Queens 385-4011
Joyce Tracking Phone calls Ref# acct receivable 3133006
Sue - Coming up for test

18 Motel 6 798-0728
Vagabond 735-01768
735 9138

Don't know why 818 VanNuys # Come up out of room???

GOODRICH INVESTIGATIONS
FACSIMILE TRANSMISSION

To: Eddie Munoz
Company:
City/State:
Fax:#:
Tel #:
Date: 4-21-01
Sender: Bert Goodrich

GOODRICH INVESTIGATIONS
2914 Ashby Avenue
Las Vegas, Nevada 89102
(702) 877-9149
FAX- (702) 878-9581

MESSAGE:
Per Our Conversation

THIS MESSAGE IS INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR ENTITY TO WHICH IS ADDRESSES AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, CONFIDENTIAL, AND EXEMPT FROM DISCLOSURE UNDER APPLICABLE LAW. IF THE READER OF THIS MESSAGE IS NOT THE INTENDED RECIPIENT OF THE EMPLOYEE OR AGENT RESPONSIBLE FOR DELIVERING THE MESSAGE TO THE INTENDED RECIPIENT. YOU ARE HEREBY NOTIFIED THAT ANY DISSEMINATION, DISTRIBUTION, OR COPYING OF THIS COMMUNICATION IS STRICTLY PROHIBITED. IF YOU HAVE RECEIVED THIS COMMUNICATION IN ERROR, PLEASE NOTIFY US IMMEDIATELY BY TELEPHONE AND RETURN THE ORIGINAL MESSAGE TO US AT THE ABOVE ADDRESS VIA THE U.S. POSTAL SERVICE. THANK YOU.

CONFIRMED BY: TIME:
Total Number of Pages (including coversheet): 4

IF YOU DO NOT RECEIVE ALL OF THE PAGES TRANSMITTED, PLEASE CALL (702) 877-9149

Attorney Work Product
Memo of Interview – MUNSRC2A WPD

Date: 4/13/01

Time: 8:30 PM

Place: Las Vegas, NV

Present: Source 2 – Witness
Bert Goodrich – Investigator

In re: Diverted Phone calls of Eddie Munoz

Source 2 provided the following information:
1. Source 2 has been in the outcall business for about 9 years.

2. Source 2 was a manager when working for Vince Bartello at Room Service

3. Source 2 explained the following scenario is common for Room Service.

A. First of all a customer (usually male) will call in from some hotel or motel. The person from Room Service gets the name of the Hotel or Motel. The guy is asked how much he wants to spend, for sake of this example let's say its $125. A girl entertainer is sent to the room.

B. When the girl gets to the room, if the guy says he only has $125 then the girl will take the $125. She then calls Room Service and tells them they they will have to send "Cody" or "Daphne". The girl then gives the phone to the customer and while he is taking with the manager from Room Service, the dancer leaves with the $125.

C. The manager from Room Service usually asks the guy if he want "Cody" a blonde, or "Daphne" a brunette. The men almost always pick "Cody" the blonde. The customer is then informed that "Cody" is on her way.

D. Room Service never sends "Cody"- who is a fictitious person. The customer waits and Cody never shows up.

4. This scenario with "Cody" and "Daphne" has been going on quite a few years at Room Service. This "Cody" and "Daphne" scenario is unique to Room Service.

5. Besides Room Service, Source 2 has worked at 4 other outcall businesses in Las Vegas.

6. Source 2 has never heard of the "Cody" and "Daphne" scenario happening at any outcall service other than Room Service.

7. Cody and Daphne were manager at Room Service in or around 1999. That is where the "Cody" and "Daphne" scenario originated.

8. The two current managers at Room Service that use the "Cody" and "Daphne" scenario are Erica and Jody. They work 4PM to midnight each week with Tuesdays and Wednesdays off.

9. After a customer at one of the hotels has been promised "Cody" or "Daphne", the customer will then call (or the entertainer will call) the phone number that the customer originally had for Room Service. The telephone girl after hearing the customer's request for "Cody" or "Daphne" will then give the customer the phone# for the manger.

10. When the customer calls the manager and gets Erica or Jody, they will tell the customer that a dancer was already sent to their room and there are no refunds. Sometimes the

customer will call back 9 or 10 times but never gets another dancer.

11. When Source 2 is the manager, a customer calling in for "Cody" or "Daphne" is told that another entertainer will be sent out who will dance for tips. This usually always satisfies the customer.

12. When the customer calls in to Room Service, they (the customer and Room Service) always settle on an amount that the customer will pay for the entertainer. This is called the drop rate. When the girl goes to the room to dance she has to give the entire amount of the drop rate to Room Service. So if the guy(s) in the room are only willing to pay the agreed upon drop rate, then the entertainer would make nothing. This is why the "Cody" and "Daphne" scenario is used, so the entertainers do not have to dance for nothing.

13. Vince Bartello knows this is going on and he makes a lot of money using the "Cody" and "Daphne" scenario, because he usually get the entire amount of the drop.

14. If a night is going really slow a manager may let an entertainer keep a portion of the drop, this is the only exception.

15. Source 2 says that Vince Bartello is the only outcall operator that makes the entertainer pay over the entire amount of the drop.

16. Again, Source 2, said that while working all shifts at Room Service people from Sprint kept coming to see Bartello at Room Service. She doesn't understand why these people are coming there because Source 2 believes Bartello gets his phone service through "Dynatel" or something like that.

End of Memo.

Attorney Work Product
Memo of Interview

Date: 2/17/01

Time: 8:30 PM

Place: Las Vegas, NV

Present: Source 1 – Witness
Bert Goodrich – Investigator

In re: Diverted Phone calls of Eddie Munoz

At the beginning of the interview I (Goodrich) identified myself as a private investigator working for Peter Alpert, who represents Eddie Munoz. In response to my questions Source 1 provided the following information:

1. He/she is a former employee of Vince Bartello's outcall service which is known as Room Service.

2. Source 1 explained the following scenario is common for Room Service.

A. First of all a customer (usually male) will call in from some hotel or motel. The person from Room Service gets the name of the Hotel or Motel. The guy is asked how much he wants to spend, for sake of this example let's say its $125. A girl entertainer is sent to the room.

B. When the girl gets to the room, if the guy says he only has $125 then the girl will take the $125. She then calls Room Service and tells them they they will have to send "Cody" or "Daphne". The girl then gives the phone to the customer and while he is taking with the manager from Room Service, the dancer leaves with the $125.

C. The manager from Room Service usually asks the guy if he want "Cody" a blonde, or "Daphne" a brunette. The men almost always pick "Cody" the blonde. The customer is then informed that "Cody" is on her way.

D. Room Service never sends "Cody"- who is a fictitious person. The customer waits and Cody never shows up.

3. Even if the amount that the customer wants to spend is $500 and the customer only has $500 when the girl shows. She may just show her boos then call Room Service and say she needs a free dancer so send "Cody or Daphne". Again the phone is given to the customer to make arrangements and ultimately "Cody" and/or "Daphne" do not show.

4. Source 1 has seen numerous people from Sprint come to visit Vince Bartello. They come every couple days. When the people from Sprint come to Room Service they have to identify themselves over an intercom before they can get in. This is how Source 1 knows that the people are from Sprint.

5. Once inside the Sprint employee(s) would go into Bartello's office and the door would be closed.

6. A news videotape was played for Source 1. The videotape showed clips taken after equipment was stolen from Sprint in Las Vegas. Source 1 identified 2 of the men in the clip as being Sprint employees who have visited Bartello.

End of Memo- MUNSRC1.WPD

No. 06-1222 Oct. 30, 2006

In the
Supreme Court of the United States

EDDIE PAUL MUNOZ; PRO SE,
- Petitioner

v.

CENTRAL TELEPHONE
COMPANY NEVADA; ET AL
-Respondents

On Petition for a Writ of Certiorari to the United States Court of Appeals for the 9th Circuit

APPENDIX Q-R-S-T
VOLUME 4

EDDIE PAUL MUNOZ : Pro Se
P.O. BOX 61344
LAS VEGAS, NEVADA 89160

APPENDIX Q

PGS A -218-226

UNITED STATES DISTRICT

COURT HEARING TRANSCRIPT

OF 1-24-2005 9: 35 AM

United States District Court
District of Nevada
Las Vegas, Nevada

EDDIE PAUL MUNOZ
Plaintiff
Vs.
SPRINT TELEPHONE COMPANY
Defendant

Las Vegas, Nevada
January 24, 2005
9:35 a.m.

ORAL ARGUMENT ON DEFANDANT'S MOTION TO DISMISS (#10)

THE HONORABLE ROBERT C. JONES PRESIDING
UNITED STATES DISTRICT COURT JUDGE

COURT RECORDER:
LILIA ABARCA de CARTER
U.S. District Court

TRASCRIPTION BY:
NW TRANSCRIPTS, LLC
Nevada Division
1027 S. Rainbow Blvd., Suite 148
Las Vegas, Nevada 89145-6232
(702) 395-2742

Proceedings recorded by electronic sound recording, transcript produced by transcription service.

APPEARANCES;
FOR THE PLAINTIFF: EDDIE PAUL MUNOZ, PRO PER
Post Office Box 61344
Las Vegas, Nevada 89160

FOR THE DEFENDANT: PATRICK J. REILLY, ESQ.
Hale, Lane, Peek Dennison, Howard & Anderson
2300 West Sahara, #800
Las Vegas, Nevada 89102

PROCEEDINGS BEGIN AT 9:35 A.M.

THE COURT: Munoz versus Sprint Telephone, please.

MR. REILLY: Good morning, Your Honor. Pat Reilly appearing on behalf of Central Telephone Company dba Sprint of Nevada.

MR. MUNOZ: Eddie Munoz, pro se.

THE COURT: Good Morning.

MR. REILLY: Good morning, Your Honor. This is Sprint's motion to dismiss the Rule 12 (b)(6) under the Rules of Civil Procedure. Mr. Martin stole my line about "it's déjà vu all over again" so I'll have to try something else. This matter goes back to 2001 and even before.

Mr. Munoz has several aspects to his business. Number one, he is a publisher. He operates a number of newspaper vending machines up and down the Strip and throughout the city except he does not distribute newspapers, he distributes publications that advertise in-call and out-call services. The other part of his business is that he operates the in-call out-call service and he has what he calls independent contractors who go out and service the in-calls and out-calls.

He has alleged since going back even before 2001 that some unknown third party has been blocking or diverting calls that would be coming into Mr. Munoz' business and sending them to another business and that he has lost –

THE COURT: Now you had an actual hearing before the public Utilities Commission?

MR. REILLY: Full evidentiary hearing.

THE COURT: It wasn't just a procedural hearing, it was an evidentiary hearing.

MR. REILLY: We had over I believe two weeks of testimony. Mr. Munoz was represented by counsel at that proceeding and the PUC issued findings of fact and conclusions of law and dismissed that complaint. Mr. Munoz had the opportunity to seek judicial review under NRS Chapter 233 (b), he –

THE COURT: And how does that statute work? Within certain time period, 30 days or something?

MR. REILLY: Within 30 days if you wish to seek judicial review of an administrative decision you must do so and that's filing a lawsuit in State District Court. If you fail to do that that becomes a final operative judgment.

Mr. Munoz failed to seek judicial review so the decision of the PUC became final and biding. That's why we have a motion for res judicata and collateral estoppel. This matter has been heard before, it's been heard on the merits, it's a final decision. It operates as a judgment effectively.

We are entitled to dismissal of this case at this point in addition to the other reasons. There's no state action by Sprint under the Section 1983 claim. There's no private cause of action under Chapter 47 of the United States Code, and also Sprint has a tariff that restricts Mr. Munoz from obtaining money damages in this case. But primarily and most certainly this matter is barred by res judicata and collateral estoppel.

THE COURT: Thank You.

MR. REILLY: Thank You.

THE COURT: Munoz.

MR. MUNOZ: Good morning, Your Honor.

THE COURT: Good Morning.

MR. MUNOZ: Your Honor, if the court would allow me to read the following statement into the record for the purpose of having it become a part of the permanent record.

The petitioner would like to have the court record reflect that I am a pro se litigant without the—without the training and expertise of a trained attorney. It should further reflect the authority of the United States Supreme Court ruling *Bounds versus Smith* should apply to these

proceedings. Due to the extent of my skills in litigation being limited to written pleadings matters such as oral arguments will limit my actions. My pro se pleadings are presently made with the help of my first cousin who is also untrained in the law.

Therefore, the petitioner would like to state as follows: the defendant's motion to dismiss has been based upon the claim by the defendants of res judicata that bars the action by the petitioners from the proceedings. However, these defendants seem to have misinterpreted what holding of the court was in these cases presented by the petitioner in his answer to the defendant's motion to dismiss. If the court would at this time examine these cases – and I'd like to read this. He is sure to find that the PUC hearing is not a judicial order, it would create that -- that would create res judicata.

In the defendant's most recent response they are down to claiming that the PUC hearing is quasi-judicial. In the first argument they were firm that the standing of PUC (sic) order had full authority of a judicial proceedings. Your petitioner has once again been left with the burden of having to interpret the rulings for the defendants. Surely he does not think that the telecommunication Act is with less authority than a PUC or state court order.

The petitioner has proof that the defendant's phone lies that were sold to the petitioner had been compromised ad remain unsecured. My claim that went before the PUC was improperly decided resulting in dismissal.

I further believe that I have a right in federal court to have the findings reviewed pursuant to the authority to the district court. Excuse me. For the standard and review under arbitrary and capricious see *Southwestern Bell versus the PUC Utilities Commission*, 28 F.2d 45 Fifth 2000.

The court in *Pacific Bell versus PacWest Telecommunication, Inc*., 325 Federal Procedures 2d, 1114 Ninth Circuit, [unintelligible] 2000 address the force of law of the PUC rulings. And I'd like to read that.

"Under the Act there has been no delegation to the state commissions of power to fill gaps in the statue through binding rule making. State commissions have been given only the power to resolve issues in arbitration and to approve or reject interconnection agreements, no to issue rulings having the force of law beyond the relationship of parties to the agreement."

THE COURT: The problem with those cases, Mr. Munoz, is as he pointed out in his reply is that they don't apply here. We're talking about an intrastate issue the PUC clearly has authority over. If it's interstate, that is from one state to another or between companies, for example, that handle traffic interstate, then the federal statute governs it preempts. But here we're talking about intrastate When I have dealings with my own telephone company intrastate, I'm under the authority of the PUC.

MR. MUNOZ: Well, at the time of the hearing and stuff it was improperly reviewed ad nobody rebutted my information. I mean there was a lot of information that I wasn't allowed to have their officers –

THE COURT: Why didn't you file a cause of action then in court within the 30-day—

MR. MUNOZ: Because at the very beginning of this I didn't want to go to the PUC because of the political magnitude of Sprint against a sole person. I waned to go into federal court but I had to exhaust my administrative remedies before I could go in the federal court.

THE COURT: That's correct, you did.

MR. MUNOZ: And at the time it was just—

THE COURT: But my question still remains, why didn't you file then a law suit within the 30 days required by statute?

MR MUNOZ: It was felonious to waste anybody's more time in that. They had – I was financially ruined at the time. I had lost my family. I had been through so many obstacles it was just unbelievable but—

THE COURT: You were represented by an attorney before the PUC?

MR. MUNOZ: Yes, and I couldn't afford to pay him anymore. There was issues where they just—I mean it was just continuing to just break my back.

THE COURT: Mr. Munoz, quite frankly that's the answer to the question. You had the opportunity. The state statute provided you a method. Your failure to exhaust in state court or in state proceedings was the fact that you failed to file a judicial proceeding either in state court or here within that 30 days. It made that decision of the PUC final. That's the problem you face.

MR. MUNOZ: Okay. Well, I would like to put in my notice for appeal to go to the Ninth Circuit.

THE COURT: Certainly.

MR. MUNOZ: And—

THE COURT: You have a time period to file a notice of appeal, sir.

I am going to grant this motion; I'll ask counsel to prepare the order. I'm granting it number one, that cause of action one and two are barred by res judicata. That is there's a prior PUC quasi-judicial ruling after a full hearing on evidence, not just a procedural ruling. They took the evidence, you were represented by counsel, you had a full opportunity to litigate that issue. You failed to file a state court action or a federal court action within 30 days prescribed by statute. Therefore, you failed to exhaust under state law.

And third and fourth, third, that you do not have a private right of action. I've reviewed the cases. There's really not much help there, but it seems that there is no private right of action under Title 47, U.S. Code, 258 and [unintelligible].

MR. MUNOZ: Finally—

THE COURT: As you've said yourself, the 1983 action was not as important to you and I think you recognize as I do that there is no state action, no under color of law action by Sprint in that proceeding. So.

MR. MUNOZ: What does a consumer do? I mean this problem continues, I still—

THE COURT: If it's intrastate, like I say, what a consumer does is you file an action with the PUC. You

litigate it. If they – if their procedures lack due process or if their ruling is unfair then you bring your lawsuit either in state or federal court within the time prescribed by statute. If it's an interstate issue then you have to – it's the state statute that governs the PUC does have authority. The federal government or court do not have authority to interfere with that.

MR. MUNOZ: And, Your Honor – I understand.

THE COURT: If I'm wrong of course you – the appellate court will correct me.

MR. MUNOZ: You know, this is a – an ongoing problem that exists for the community. I mean I'm not the only person, you know. I mean my rights were denied, I mean - - to my Fifth and Fourteenth Amendments were violated during that hearing. I wasn't able to bring officers that wanted to testify during the – with the Homeland Security issues with our, you know, Las Vegas being a number one target in the United States.

THE COURT: The answer to that, Mr. Munoz, is very simply if they made a mistake – if the PUC made a mistake in their rulings, in the way they handled the hearing, you've got to bring a lawsuit timely.

MR. MUNOZ: Okay. So I man if I file another complaint I mean back at the door again.

THE COURT: That could be.

MR. MUNOZ: Okay.

THE COURT: Okay.

MR. MUNOZ: Well, I'll see you again, sir.

THE COURT: Thank You.

MR. REILLY: Thank You, Your Honor, I'll prepare the order.

THE COURT: Thank You. Thank you and thank you for your time.

PROCEEDINGS CONCLUDED AT 9:47 A.M.

* * * * * * * * * * *

CERTIFICATION

I (WE) CERTIFY THAT TE FOREGOING IS A CORRECT TRANSCRIPT FROM THE ELECTRONIC SOUND RECORDING OF THE PROCEEDINGS IN THE ABOVE-ENTITLED MATTER.

NW TRANSCRIPTS, LLC
NEVADA DIVISION
1027 S. RAINBOW BLVD., #148
LAS VEGAS, NEVADA 89145-6232
(702) 395-2742

(s)_____
FEDERALLY CERTIFIED MANAGER/ OWNER

Kay McCrea_____
TRANSCRIBER

2/4/05_____
DATE

APPENDIX R

PGS 227-242

SPRINT TROUBLE TICKETS

SHOW PROBABLE CAUSE

PROBLEM EXISTS UP TO DATE

Intrusion Detection

High stakes= high risk

Overview

Generating revenue is never put on the back burner, and neither should your network security system. How valuable is effective network security to your company? A single access breach can cost $1.41 million according to the CSI/FBI 2004 Computer Crime and Security Survey.*

Don't let a network intrusion go unnoticed. Get a effective, managed security solution that includes network-based intrusion detection service to go hand-in hand with your firewall protection. While firewalls keep out bad network traffic. Sprint intrusion Detection Services (IDS) safeguards your network by monitoring incoming traffic and warning against unauthorized access attempts. Sprint IDS solutions can log intrusion information around the-clock, giving you the warning you need to react quickly and protect your intellectual assets.

*CSI/FBI 2004 Computer Crime and Security Survey based on 269 respondents.

http://www.sprint.com/business/products/products/intrusionDetection.jsp

11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-431-6722**
Sprint Ticket Number: **2585415**
Problem Type: **(Hear Conversation In Background/Cannot Communicate With Party) Noise**
Clear Date/Time: **04/01/2005 – 12:00**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **9937616**
Problem Type: **(Hear Conversation In Background/Cannot Communicate With Party) Noise**
Clear Date/Time: **10/08/2004 – 17:57**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **0501430**
Problem Type: **(Double Connection While Talking) Miscellaneous**
Clear Date/Time: **11/02/2004 – 15:17**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **0559627**
Problem Type: **(Callers Reach Busy – No One On Line) Can't Be Called**
Clear Date/Time: **11/08/2004 – 16:07**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **0965044**
Problem Type: **(Reach Recording) Miscellaneous**
Clear Date/Time: **12/14/2004 – 09:34**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **1869214**
Problem Type: **(Callers Reach Busy – No One On Line) Can't Be Called**
Clear Date/Time: **02/13/2005 -11:45**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number:**1887007**
Problem Type: **(Callers Reach Busy- No One On Line) Can't Be Called**
Clear Date/Time: **02/14/2005 – 15:17**
Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **2585362**
Problem Type: **(Hear Conversation in Background/Cannot Communicate With Party) Noise**
Clear Date/Time: **04/01/2005 - 11:30**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **2617191**
Problem Type: **(No Audible Ring) Can't Call**
Clear Date/Time: **04/03/2005 – 14:53**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **2641994**
Problem Type: **(Noisy) Noise**
Clear Date/Time: **04/05/2005 – 11:13**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **2646146**
Problem Type: **(Noisy) Noise**
Clear Date/Time: **04/06/2005 – 09:15**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **2846634**
Problem Type: **(Other) Feature**
Clear Date/Time: **04/26/2005 – 13:15**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **9937616**
Problem Type: **(Hear Conversation in Background/ Cannot Communicate/ With Party) Noise**
Clear Date/Time: **10/05/2004 – 17:57**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-440-6441**
Sprint Ticket Number: **2642155**
Problem Type: **(Noisy) Noise**
Clear Date/Time: **04/05/2005 – 10:05**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-440-6441**
Sprint Ticket Number: **2646282**
Problem Type: **(Noisy) Noise**
Clear Date/Time: **04/06/2005 – 11:00**
Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_ce
nter/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-440-6441**
Sprint Ticket Number: **2879169**
Problem Type: **(Other) Feature**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_ce
nter/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-440-6441**
Sprint Ticket Number: **3516611**
Problem Type: **(No Dial Tone) Can't Call**
Clear Date/Time: **06/07/2005 -17:52**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-440-6441**
Sprint Ticket Number: **2585435**
Problem Type: **(Hear Conversation in Background/Cannot Communicate With Party) Noise**
Clear Date/Time: **04/01/2005 – 12:30**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-432-2333**
Sprint Ticket Number: **2617244**
Problem Type: **(No Audible Ring) Can't Call**
Clear Date/Time: **04/03/2005 – 14:51**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-432-2333**
Sprint Ticket Number: **2642213**
Problem Type: **(Noisy) Noise**
Clear Date/Time: **04/5/2005 – 10:40**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-432-2333**
Sprint Ticket Number: **2646236**
Problem Type: **(Noisy) Noise**
Clear Date/Time: **04/06/2005 – 09:50**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-432-2333**
Sprint Ticket Number: **2881641**
Problem Type: **(Hear Conversation in Background/ Cannot Communicate With Party) Noise**
Clear Date/Time: **05/1/2005 – 16:30**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-432-2333**
Sprint Ticket Number: **2585422**
Problem Type: **(Hear Conversation in Background/Cannot Communicate With Party) Noise**
Clear Date/Time: **04/01/2005 – 10:30**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-440-6441**
Sprint Ticket Number: **2585435**
Problem Type: **(Hear Conversation in Background/Cannot Communicate With Party) Noise**
Clear Date/Time: **04/01/2005 – 12:30**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-432-2333**
Sprint Ticket Number:**2585422**
Problem Type: **(Hear Conversation in Background/Cannot Communicate With Party) Noise**
Clear Date/Time: **04/01/2005 – 10:30**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-431-6722**
Sprint Ticket Number: **2646262**
Problem Type: **(Noisy) Noise**
Clear Date/Time: **04/06/2005 – 10:25**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-431-6722**
Sprint Ticket Number: **2585415**
Problem Type: **(Hear Conversation In Background/ Cannot Communicate With Party) Noise**
Clear Date/Time: **04/1/2005 - 12:00**
Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-431-6722**
Sprint Ticket Number: **2617222**
Problem Type: **(No Audible Ring) Can't Call**
Clear Date/Time: **04/3/2005 - 14:55**
Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

APPENDIX S

PGS-A- 243-253

EMBARQ TROUBLE TICKETS

SHOW PROBABLE CAUSE

SHELL GAME

PROBLEM EXISTS UP TO DATE

Embarq Local Business / Work Order Detail

View Ticket History EMBARQ Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **8742128**
Problem Type: **(Other) Feature**
Clear Date/Time: **05/19/2006 – 13:57**

Contact Sprint with questions about this work order.

© Embarq Holdings Company LLC. All rights reserved.
The name EMBARQ and the jet logo are trademark of
Embarq Holdings Company LLC.

https://managebusiness.embarq.com/bizpark/page/service_
center/small_office/view_histor... 10/6/2006

Embarq Local Business / Work Order Detail

View Ticket History EMBARQ Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **9448526**
Problem Type: **(No Dial Tone) Can't Call**
Clear Date/Time: **06/28/2006 – 12:10**

Contact Sprint with questions about this work order.

© Embarq Holdings Company LLC. All rights reserved.
The name EMBARQ and the jet logo are trademark of
Embarq Holdings Company LLC.

https://managebusiness.embarq.com/bizpark/page/service_
center/small_office/view_histor... 10/6/2006

Embarq Local Business / Work Order Detail

View Ticket History EMBARQ Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **9466839**
Problem Type: **(No Dial Tone) Can' Call**
Clear Date/Time: **06/29/2006 – 08:45**

Contact Sprint with questions about this work order.

© Embarq Holdings Company LLC. All rights reserved.
The name EMBARQ and the jet logo are trademark of
Embarq Holdings Company LLC.

https://managebusiness.embarq.com/bizpark/page/service_
center/small_office/view_histor... 10/6/2006

Embarq Local Business / Work Order Detail

View Ticket History EMBARQ Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **9478017**
Problem Type: **(Callers Reach Busy – No One On Line) Can't Be Called**
Clear Date/Time: **06/29/2006 – 16:00**

Contact Sprint with questions about this work order.

© Embarq Holdings Company LLC. All rights reserved.
The name EMBARQ and the jet logo are trademark of
Embarq Holdings Company LLC.

https://managebusiness.embarq.com/bizpark/page/service_
center/small_office/view_histor... 10/6/2006

Embarq Local Business / Work Order Detail

View Ticket History EMBARQ Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **9873610**
Problem Type:
Clear Date/Time: **07/30/2006 – 15:03**

Contact Sprint with questions about this work order.

© Embarq Holdings Company LLC. All rights reserved.
The name EMBARQ and the jet logo are trademark of
Embarq Holdings Company LLC.

https://managebusiness.embarq.com/bizpark/page/service_
center/small_office/view_histor... 10/6/2006

Embarq Local Business / Work Order Detail

View Ticket History EMBARQ Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **9993389**
Problem Type: **(Hear Conversation In Background/ Cannot Communicate With Party) Noise**
Clear Date/Time: **08/08/2006 – 9:10**

Contact Sprint with questions about this work order.

© Embarq Holdings Company LLC. All rights reserved.
The name EMBARQ and the jet logo are trademark of
Embarq Holdings Company LLC.

https://managebusiness.embarq.com/bizpark/page/service_
center/small_office/view_histor... 10/6/2006

Embarq Local Business / Work Order Detail

View Ticket History EMBARQ Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **0891275**
Problem Type: **(No Dial Tone) Can't Call**
Clear Date/Time: **09/29/2006 – 10:45**

Contact Sprint with questions about this work order.

© Embarq Holdings Company LLC. All rights reserved.
The name EMBARQ and the jet logo are trademark of
Embarq Holdings Company LLC.

https://managebusiness.embarq.com/bizpark/page/service_
center/small_office/view_histor... 10/6/2006

Embarq Local Business / Work Order Detail

View Ticket History EMBARQ Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **5812945**
Problem Type: **(Noisy) Noise**
Clear Date/Time: **10/26/2005 – 17:37**

Contact Sprint with questions about this work order.

© Embarq Holdings Company LLC. All rights reserved.
The name EMBARQ and the jet logo are trademark of
Embarq Holdings Company LLC.

https://managebusiness.embarq.com/bizpark/page/service_
center/small_office/view_histor... 10/6/2006

EMBARQ™

Sign Off

Trouble Ticket Search

This service is only available to customers who have previously opened a ticket. If you need additional assistance, please visit Support. To review ticket status, please enter your ticket number and click Search.

Trouble Ticket Search

Look up Ticket

Ticket Number:
SEARCH
Phone Number: 702-440-6441
SEARCH

Ticket Status Info

Ticket Status: Closed

Ticket Detail Info

Ticket Number: 9466949

Ticket Created Date and Time: 06/28/2006 at 01:34 PM PST

Problem Type: (No Dial Tone) Can't Call

Embarq Committed Date & Time: 06/29/2006 at 12:30 PM PST

Customer & Service Address/Location Info

Problem Phone #: 7024406441

Address: 4372 E. BOSTON AVE
City: LAS VEGAS
State: Nevada
ZIP: 891045308

Ticket Service Charge Info

Service Charge Description: 0.00 Customer has LineGuard. No trouble isolation charge or incremental charges to repair inside wiring or jacks.

Service Charge Status: Advised

Ticket Closing Info

Closing Date & Time: 06/29/2006 at 09:04 AM PST

Contact Us: If you would like to contact Embarq regarding this ticket or would like to cancel this ticket, click on the link directory below. Please provide the reason for canceling any ticket.

Contact Embarq regarding this ticket

© 2006 Embarq Holdings Company LLC. All Rights Reserved. The name EMBARQ and the jet logo are trademarks of Embarq Holdings Company LLC.

EMBARQ™

Sign Off

Trouble Ticket Search

This service is only available to customers who have previously opened a ticket. If you need additional assistance, please visit Support. To review ticket status, please enter your ticket number and click Search.

Trouble Ticket Search

Look up Ticket

Ticket Number:
SEARCH
Phone Number: 702-432-2333
SEARCH

Ticket Status Info

Ticket Status: Closed

Ticket Detail Info

Ticket Number: 9467045

Ticket Created Date and Time: 06/28/2006 at 01:38 PM PST

Problem Type: (No Dial Tone) Can't Call

Embarq Committed Date & Time:
06/29/2006 at 12:40 PM PST

Customer & Service Address/Location Info

Problem Phone #: 7024322333

Address:	4372 E. BOSTON AVE
City:	LAS VEGAS
State:	Nevada
ZIP:	891045308

Ticket Service Charge Info

Service Charge Description: 0.00 Customer has LineGuard. No trouble isolation charge or incremental charges to repair inside wiring or jacks.

Service Charge Status: Advised

Ticket Closing Info

Closing Date & Time: 06/29/2006 at 09:04 AM PST

Contact Us: If you would like to contact Embarq regarding this ticket or would like to cancel this ticket, click on the link directory below. Please provide the reason for canceling any ticket.

Contact Embarq regarding this ticket

© 2006 Embarq Holdings Company LLC. All Rights Reserved. The name EMBARQ and the jet logo are trademarks of Embarq Holdings Company LLC.

EMBARQ™

Sign Off

Trouble Ticket Search

This service is only available to customers who have previously opened a ticket. If you need additional assistance, please visit Support. To review ticket status, please enter your ticket number and click Search.

Trouble Ticket Search

Look up Ticket

Ticket Number:
SEARCH
Phone Number: 702-431-6722
SEARCH

Ticket Status Info

Ticket Status: Closed

Ticket Detail Info

Ticket Number: 9992545

Ticket Created Date and Time: 08/07/2006 at 03:09 PM PST

Problem Type: (No Dial Tone) Can't Call

Embarq Committed Date & Time: 08/08/2006 at 02:10 PM PST

Customer & Service Address/Location Info

Problem Phone #: 7024316722

Address: 4372 E. BOSTON AVE
City: LAS VEGAS
State: Nevada
ZIP: 891045308

Ticket Service Charge Info

Service Charge Description: 0.00 Customer has LineGuard. No trouble isolation charge or incremental charges to repair inside wiring or jacks.

Service Charge Status: Advised

Ticket Closing Info

Closing Date & Time: 08/08/2006 at 10:54 AM PST

Contact Us: If you would like to contact Embarq regarding this ticket or would like to cancel this ticket, click on the link directory below. Please provide the reason for canceling any ticket.

Contact Embarq regarding this ticket

© 2006 Embarq Holdings Company LLC. All Rights Reserved. The name EMBARQ and the jet logo are trademarks of Embarq Holdings Company LLC.

APPENDIX T

PGS A-254-269

NATIONAL SECURITY ISSUE'S

CYBER WAR

SECURING SS7

TELECOMMUNICATION NETWORKS

**Proceedings of the 2001 IEEE
Workshop on Information Assurance and Security
United States Military Academy, West Point, NY, 5-6
June 2001**

Securing SS7 Telecommunications Networks

G. Lorenz, T. Moore, G. Manes, J. Hale, S. Shenoi*

Abstract---Signaling System 7 (SS7) defines the network architecture, configuration and message transport protocol for Public Telephone Network (PTNs). SS7 was originally designed for a closed telecommunications community, and therefore possesses limited authentication facilities. Deregulation coupled with PTN convergence with the Internet enabling attackers to perpetrate fraud, interception and interruption on a potentially massive scale.

This paper analyzes vulnerabilities in SS7 networks and presents an attack taxonomy. The architecture of a system for detecting and responding to SS7 network attacks is also described.

Keywords--- Public telephone networks, SS7 networks, vulnerabilities, critical infrastructure protection

I. INTRODUCTION

Public Telephone Networks (PTNs) are massive heterogeneous networks comprising three overlapping sub-networks: a PTN backbone, the Internet and wireless networks [4,9,13]. The PTN backbone employs signaling, transmission and operations equipment. Signaling equipment sets up and tears down calls; it includes databases and adjunct processors for number translation and call routing. Transmission equipment carries the actual telephone conversation. Operations equipment, including the operations support system (OSS), performs

management, inventory, engineering and repair functions [12].

The older in-band signaling technique combined signaling and transmission over "homerun" copper wires. But this solution was inefficient and did not support advanced PTN service [2]. The newer-and widely used – out of-band signaling separates voice transmission from the data that manage calls. Out-of-band communication between central-office switches occurs via dedicated (private and public) X.25 data networks using special protocols, most notably Signaling System 7 (SS7), to set up calls, establish billing and return busy signals [2,12].

The global standard for telecommunications, SS7 defines procedures by which PTN elements exchange information over a digital signaling network. The SS7 standard governs network architecture, configuration and message transport. The network architecture supports base communications, routing and database access across PTNs. Dedicated out-of-band SS7 networks also help prevent in-band fraud while conserving telecommunications resources.

Although SS7 reduces in-band attacks, it introduces other vulnerabilities [8,11]. The protocol was originally designed for a closed telecommunications community; therefore, it possesses limited authentication facilities. However, deregulation now requires phone companies to provide SS7 connections to any entity for a modest fee. The Internet-PTN convergence allows attackers inroads via entities with poorly secured SS7 networks. ISDN connections are also points of unauthorized entry.

Once access to a PTN is gained, an attacker can perpetrate modification, fabrication, interception on a potentially massive scale. For example, during a terrorist bombing incident, an attacker can modify entries in a call-forwarding database to re-route all phone calls to emergency services, disrupting them and possibly increasing the number of casualties.

Very few systems exist for securing SS7 networks. Secure Logix produces Telewall, a firewall for private branch exchanges (PBXs) that controls unauthorized

access [14]. Sevis Systems has developed the Intele Guard Signaling Firewall for controlling access to central office switches [15]. Apart from these efforts, published research on defending SS7 networks against attacks is virtually non-existent.

This paper focuses on the problem of securing SS7 networks. The SS7 architecture and protocol are described, and their vulnerabilities are analyzed in detail. Taxonomy of attacks on SS7 networks is presented, and the architecture of a system for systematically detecting and responding to these attacks is described.

II. SIGNALING SYSTEM 7 (SS7) NETWORK

Public Telephone Networks (PTNs) typically are composed of a PTN backbone, the Internet and wireless networks (Figure 1) [4,9]. The PTN backbone primarily uses the Signaling System 7 (SS7) protocol, the Internet employs the TCP/IP protocol suite, and wireless networks use the CDMA, TDMA and GSM protocols [5,7]. As shown in Figure 1, the PTN backbone is connected to the Internet and wireless networks via IP and wireless gateways, respectively. In addition, the PTN backbone maintains diverse connections to entities ranging from large organizations to individual users. For example, individuals and small organizations use xDSL, Dialo-Up and ISDN connections to access the PTN (or Internet) [6]. Large organizations employ analog trunks to connect PBXs (Private Branch Exchanges) to the PTN.

The SS7 network controls many PTN features, e.g., basic call setup, management, tear down, billing and returning busy signals. It also supports advanced services such as local number portability (LNP), toll-free (800/888) and toll (900) services. Enhanced call features such as call forwarding, calling party name/number display, and three-way calling are also controlled. SS7 not only facilitates these and other new services, but also provides a more efficient and secure telecommunications network.

The SS7 standard defines the signaling architecture and protocols employed for message transport. This section describes these components in detail.

A. SS7 Architecture

The SS7 architecture comprises three signaling points: service-switching points (SSPs), signal transfer points (STPs) and service control points (SCPs) (Figure 2). Each signaling point is identified by a unique point code that facilitates the routing of signaling messages. Signaling points are connected via signaling links, typically 56 or 64 kbps bi-directional X.25 data links. SSPs are the entry and exit points for SS7 networks, i.e., they strictly originate, terminate and tandem telephone calls. They are analogous to border routers on the Internet and are the primary entry points for attackers.

Figure 2 shows an SSP (1) connected to two pairs of STPs via access (A) links, the primary channels for all STPs-SSP communications. A links simultaneously support up to 9600 connections [12]. If the number of connections exceeds 9600, the SSP diverts traffic to extended (E) links (shown connecting SSP (1) to an alternative STP in Figure 2). The architecture does not demand that SSPs be deployed with E links. Therefore, some SSPs, e.g., SSP (2) in Figure 2, cannot handle large volumes of traffic. SSPs communicate by sending signaling messages over A and E links to other SSPs via STPs. They send queries to SCPs via STPs using separate links.

Figure 2 shows the four primary line types connecting SSPs to end users: analog lines, ISDN lines, X.25 data lines and leased lines. Voice trunks are analog lines directly connected to SSPs. Analog signals received by SSPs are converted to digital signaling messages to handle the call. ISDN lines represent the next stage of PTN evolution by removing analog signals from the loop [1]. These connections contain a digital (D) channel that generates digital signaling messages (resembling SS7 packets) at customer telephones, interfacing directly to

SSPs. The C channel of an ISDN connection architecturally resembles the X..25 connections used by competitive local exchange carriers (CLECs), typically small start-up companies offering services ranging from long distance to voice mail [12]. In addition, much of the Internet is connected to SSPs via leased lines. Therefore, all data passing over these lines passes through SSPs.

Once a call has been initiated by an SSP, it is routed using a matching set of STPs. All SSPs are connected to at least one mated pair of STPs. STPs are the routers of a PTN, receiving and then routing SS7 network traffic between signaling points. Messages to outside destinations must travel through dedicated STPs. STPs facilitate database access by detecting and routing queries to SCPs. They also conned call requests between SSPs. As shown in Figure 2, STPs often link to the operations support systems (OSSs), remote maintenance centers that monitor and manage PTNs. Using signaling links, OSSs connect to STPs, introducing SS7 messages throughout the PTN.

SCPs provide database access needed for advanced services. They directly connect to STPs (like SSPs). SCPs respond to queries with information necessary to process calls, accessing information sources that maintain consumer and call information, including call management service databases (CMADBs), local number portability (LNP) and line information databases (LIDBs) [12].

B. SS7 Protocol

The SS7 protocol defines the procedures for operating and communicating over SS7 networks. The protocol resembles the popular OSI model (see Figure 3). [12]. The SS7 message transfer part (MTP) Levels 1-3 correspond directly to the physical, data link and network layers of the OSI model. The user and application parts of the SS7 protocol loosely correspond to OSI Layers 4-7; they detect the connection/disconnection protocol and the remote database access protocol.

MTP Level 1 defines the electrical characteristics of signaling links and the types of interfaces used in the network, i.g., Digital Signal O (DSOA) and V.35. DSOA is a 56/64 kbps channel within a DS1 (1.544 Mbps) facility, often used in ISDN networks and T-1 trunks [12]. DSOAs are the most commonly used interfaces in the United States. V.35 interfaces also support 56/64 kbps links, but they were designed to interface analog modems with digital lines and are no longer recommended.

MTP Level 2 ensures the sequenced delivery of all SS7 messages and provides the tools necessary for reliable transport throughout the network. MTP Level 3 routes and distributes messages to the proper destinations. Using routing tables that store point codes, the routing function finds the correct destination point codes and delivers he messages. Link, routing and traffic management of netw3ork elements all occur at the network level. Link management oversees the error levels at each link and sends messages advising of a link's failed or restored status. In cooperation with link management, routing management notifies other signaling points about the failure, and only re-routes those signals that are affected by the failure. The similarities between the SS7 and OSI protocols fade at this point.

Once MTP ensures reliable signaling between adjacent nodes, SS7-specific protocols define cross network communications such as telephone call connections, disconnections and remote function control. The ISDN user part (ISUP) provides connection-oriented services in SS7 networks, setting up and tearing down circuits for voice and data between exchanges [1,12]. ISUP also offers supplementary services for the circuits carrying the transmission, e.g., sending caller information between the end points during calls. International networks employ the telephone user part (TUP) to handle call setup and teardown. TYP is compatible with ISUP, but it does not facilitate the needs of modern digital networks, especially advanced services. Consequently, ISUP is the predominant protocol while TUP is being phased out worldwide.

The signaling connection control part (SCCP) provides connectionless and connection-oriented services, although it has only been implemented for connectionless services. While MTP provides routing between adjacent nodes, SCCP performs end-to-end routing for the transaction capabilities application part (TCAP) protocol. TCAP employs SCCP connectionless service to transport non-circuit related information between signaling points. End users in the SS7 network use TCAP for peer-to-peer communication. Since TCAP allows signaling points to remotely access each other, TCAP also supports database access. In addition, SCCP enables STPs to provide global title translation, i.e., allow originating messages to only indicate general digits, not point codes. Subsequently, STPs use SCCP to transport messages to their destinations, effectively preventing outsiders from obtaining internal network point codes.

III. SS7 NETWORK VULNERABILITIES

Major SS7 network vulnerabilities, as with the Internet, arise from the number and complexity of interfaces between distinct SS7 entities. Moreover, advanced services like call forwarding have intrinsic vulnerabilities-attackers can create havoc by modifying SCPs containing forwarding destinations.

Additional vulnerabilities arise from the increasing inter-dependence and interconnectivity between SS7 networks and the Internet [4,6,9]. Large portions of the Internet use leased phone lines. Conversely, SS7 systems are networked using Internet technologies, and often, the Internet itself. Thus, SS7 vulnerabilities can affect the Internet, and Internet vulnerabilities can affect SS7 networks. Furthermore, SS7 incorporates limited authentication procedures (because it was originally designed for a closed telecommunications community). Consequently, anyone capable of generating SS7 messages and introducing them into a network can disrupt PTN services. Figure 2 identities potential entry points for attacks (Attackers 1,2, and 3)

. Users with ISDN connections can introduce digital messages into the SS7 network [1]. Attacker 1 in Figure 2 exploits this relationship by spoofing the source telephone number and introducing malicious packets onto the network. Additionally, PTN-Internet convergence gives Attacker 2 new entry points to the network. While large regional Bell operating companies (RBOCs) have significant security staff and resources, competitive local exchange carriers (CLECs) – typically small startup companies – often have limited budgets and may be relatively insecure. Thus, Attacker 2 can gain access to SSPs by compromising networked computers at a CLEC.

The Telecommunications Act of 1996 grants an SS7 network connection to any entity (including a possibly malicious one) for a modest fee (currently $10,000) [13]. Traffic on SS7 networks is therefore suspect (Attacker 3 in Figure 2).

Because STPs and SCPs use front-end computer systems, hacker exploits that seize control of netrwork operating systems pose serious threats. Local number portability (LNP), another service mandated by the 1996 Telecommunications Act, allows telephone users to switch local providers without having to change telephone numbers. LNP is another point of vulnerability. Once access is gained to SS7 networks, attackers have it easy. Virtually no systems exist for detecting and responding to attacks.

A. SS7 Attack Taxonomy

The vulnerabilities described in the previous section entitled a slew of attacks on SS7 networks. An attack taxonomy is presented on Figure 4. The targets are SSPs, STPs and SCPs. Four types of attacks are attacks are possible: modification, interception, interruption and fabrication [10].

B.SSP Attacks

SSPs constitute the SS7 network perimeter and are the gateways for attack. Most attacks exploit SS7's weak

authentication. For example, ISDN was designed to connect the edges of SS7 networks to end users, enabling ISDN users to introduce traffic directly into an SS7 network [1]. Malicious ISDN connections used by CLECs. ISDN connections, however, are available at a much lower cost (less than $100 per month).

All SS7 network elements are susceptible to packet sniffing. However, an SSP is a prime target for sniffing specific users, because each user's traffic must flow through the corresponding SSP. Attackers can also intercept services intended for a user by appending the attacker's destination to the original destination in the message.

SSPs, like all network elements, have a maximum operating capacity. Overloading an SSP-STP connection can interrupt SSP service, denying service to a segment of users. For example, one distributed denial of service (DDoS) attack introduces large numbers of initial address messages (IAMs, i.e., ISUP messages that start call setups) and direct them at a single SSP. Attackers could also intercept all traffic at a compromised signaling point, and modify IAMs to request connections with a targeted user on the same SSP. Since message sources of ISUPs can be spoofed quite easily, SSPs cannot trace the sources of such attacks.

C. STP Attacks

STPs perform routing and all messages must pass through them. Therefore, attacks that exploit routing protocols are a major concern.

SSP traffic travels directly through STPs. Thus, attackers who compromise an STP can view all traffic to and from the corresponding SSPs. A more sophisticated attack remotely compromises an STP, and then creates a transparent bogus STP that filters traffic and re-routes it to the STP. Thus, it is possible to eavesdrop on selected conversations. Modifying the destinations of SCCP (end-to-end) messages allow corresponding telephone calls (and database queries) to be re-routed at will.

Since OSSs connect to STPs, toll fraud can be perpetrated by seizing control of the OSS via the STP. Global title digits are the digits provided by the called party address. These digits do not give the point code or subsystem number, although SCCP translates the global title digits to the appropriate point code. SCCP messages with a global title (i.g., 800 numbers) must be routed through an STP, which then translates the global title to the actual point code, usually an SCP. Points codes are sensitive information, and global title translation protects the information by requiring an originating message to only provide general information that the STP can then translate to specific point codes. However, if an STP is compromised, the point codes of internal network nodes con be determined by accessing the corresponding SCPs. Another attack can modify the global title translation database maintained within the STP.

As with all routers, STPs can be overloaded with traffic, although, this is more difficult because STPs are usually deployed in redundant mated pairs. Denial of service attacks are still be possible, however, if multiple SCP databases are modified to re-route large numbers of calls to telephone numbers on a specific SSP. Additionally, an attacker compromising multiple STPs could re-route all received messages to a target STP, in effect, overloading the STP and rendering the connected SSP useless.

The OSS is susceptible to traditional computer attacks. These include viruses, worms and Trojan horses since the Oss is typically a collection of computers.

STPs and SCPs maintain local number portability (LNP) databases that hold information for routing calls. Queries of LNP databases require considerable system resources. Therefore, LNP overload is a real threat-an attacker generating massive amounts of LNP queries can shut down STPs and/or SCPs maintaining the LNP databases. Additionally, telephone numbers in LNP databases can be modified or erased.

MTP Level 3 of the SS7 protocol provides sophisticated link traffic management [11]. Message signaling units (MSUs) can notify surrounding signaling points of a node

failure, causing traffic to be re-routed around the failed node. Fabricated MSUs could render operational signaling points useless, resulting in congestion and possible crippling of the network.

D. SCP Attacks

SCP databases that store sensitive information are highly vulnerable. Consider, for example, call management services databases (CMSDBs) that process toll-free calls [12]. Toll-free numbers do not represent the actual telephone number dialed. Instead, the toll-free number is mapped to an actual telephone number and the billing information is maintained separately. The CMSDB provides routing instructions that map the call and the billing information for the call. An attacker could fraudulently change the destination number to some other number, thus re-moving all charges for calls made to destination number. Alternatively, the owner of a toll-free number could also change the billing information to void charges.

Similar modifications are possible with billing databases, LNP databases; liner information databases (LIDBs) and others. An LIDB maintains subscriber information, including billing; collect call service, calling card service and validation, and personal identification numbers (PINs). Access to this database facilitates malicious activities ranging from identity theft to toll fraud. For example, attacker could modify the billing amounts, intercept, and even modify PINs.

Many SCP attacks utilize TCAP messages that support access and modification of SCP databases. For example, an attacker could modify the subscriber account number in a TCAP message destined for an LIDB and so avoid billing. Likewise, subscribers' PINs could be obtained by generating the appropriate TCAP requests.

Voice mail databases have similar vulnerabilities. An attacker could send a TCAP message query for a certain user's password and gain full access to his/her voice mail-box.

SCP databases are also vulnerable to interruption or denial of service attacks. A compromised SCP could simply have its databases deleted, disrupting all advanced services. Additionally, a business could interrupt a competitor's toll-free number by associating it with an unrelated, even illicit, telephone number (e.g., a phone sex company.) More seriously, an attacker could modify all the destination numbers in a call-forwarding database and route them to a single number, i.g., emergency services (911), completely shutting it down.
The fabrication of TCAP messages also permits unauthorized SCP database access and modification. Such attacks can severely disrupt SS7 network services.

IV. SS7 ATTACK MANAGEMENT SYSTEM

Attack management in An SS7 network requires the coordination of diverse platforms, operating systems and applications. The subsystems and tools constituting the attack management system, currently under development, must be strategically positioned throughout the SS7 netrwork (Figure 5).

The heterogeneous, distributed architecture requires a secure communication infrastructure that provides authentication, encryption and access control mechanisms. The infrastructure employs a combination of a private (backside) network and a VPN-style public network. Secure communication will be implemented using public/private key cryptography and secure broadcasting (with capabilities).

Since SSPs represent the SS7 network perimeter, authentication modules detect attempts at spoofing and identity subversion by comparing SS7 messages with signatures of spoofing attacks.

SS7 packet sniffers, specially designed to read and interpret SS7 messages, are the primary information gatherers of the attack management system. The sniffers are positioned to passively monitor all signaling channels (Figure 5). They continuously transmit information to the other tools on the network.

SS7 firewalls are designed actively filter SS7 messages. As shown in Figure 5, they are positioned between SSPs and STPs to control traffic at all switching points. The firewalls screen traffic for attack signatures that are maintained in a special database.

SCPs interface with databases supporting advanced PTN services. Therefore, a real time fraud analyzes is located at each SCP. The analyzers examine SCP queries (TCAP messages) for suspicious patterns. For example, they check successive TCAP messages that seek to modify telephone numbers in call forwarding databases.

SCP access control modules work in conjunction with fraud analyzers. Positioned in front of SCPs to regulate entrance, the control modules determine whether or not TCAP messages destined for SCPs are "safe" based on their source data and information received from the corresponding fraud analyzer.

Each of the tools comprising the attack management system represents a systematic response to known SS7 vulnerabilities. Obviously, the tools and system will not completely secure SS7 networks. They will, however, help address many of the major problems facing modern public telephone networks.

During the fall of 1997, telephone systems in Puerto Rico were sabotaged by physically cutting lines [3]. The convergence of information and communications into a single global network makes it possible to conduct similar attacks from afar with software. Sophisticated systems are required to address a spectrum of cyber threats – ranging from emergency service disruption to coordinated strikes designed to destroy the communications infrastructure and cripple American society [16].

While substantial attention has been directed at securing computer networks, little work had focused specifically on public telephone networks (PTNs). This paper is among the first to analyze vulnerabilities in SS7 networks and present an attack taxonomy. It is hoped that this taxonomy and the system for detecting and responding to SS7 network attacks, currently under construction, will spur

efforts to develop and deploy sophisticated systems for safeguarding telecommunications networks.

ACKNOWLEDGMENTS

The research is supported by the National Institute of Justice through the Memorial Institute for the Prevention of Terrorism (MIPT), Oklahoma City, Oklahoma.

REFERENCES

[1] U. Black, ISDN and SS7: Architectures for Digital Signaling Networks, Prentice Hall, Upper Saddle River, New Jersey, 1997.

[2] J. Bosse, Signaling in Telecommunication Networks, John Wiley and Sons, New York, 1997.

[3] D. Denning, Information Warfare and Security, Addison-Wesley, Reading, Massachusetts, 1999.

[4] I. Faynberg, et al., Converged Networks and Services: Internet-working IP and the PSTN, John Wiley and Sons, New York, 2000.

[5] S. Glisic, et al., Wireless Communications: TDMAv. CDMA, Kluwer Academic Publishers, Boston, 1997.

[6] P. Kuhn, et al., Broadband Communications: Convergence of Network Technologies, Kluwer Academic Publishers, Boston, Massachusetts, 1999.

[7] Y. Lin, et al., Wireless and Mobily Network Architectured, John Wiley and Sons, New York, 2000.

[8] G. Lorenz, et al., Characterization of attacks on public telephone networks, Proceedings of the SPIE Conference on Technology on Law Enforcement, Boston, Massachusetts, November 5-8, 2000.

[9] N. Muller, IP Convergence: The Next Revolution in Telecommunications, Artech House, Norwood, Massachusetts, 1999.

[10] C. Pfleeger, Security in Computing, Prentice Hall, Upper Saddle River, New Jersey, 1997.

[11] M. Rozenblit, Security for Network Telecommunications Management, IEEE Press, Piscataway, New Jersey, 2000.

[12] T. Russell, Signaling System #7, McGraw-=Hill, New York, 2000.
[13] F. Schneider (Ed.), Trust in Cyberspace, National Academy Press, Washington, D.C., 1999.
[14] SecureLogix Corp., San Antonio, Texas (www.securelogix.com)
[15] Sevis Systems, San Antonio, Texas (www.sevis.com).
[16] The White House, Defending America's Cyberspace: National Plan for Information Systems Protection (Version 1.0), Washington, D.C., 2000.

6

06-1233 Oct. 30, 2006

No._____

In the
Supreme Court of the United States

EDDIE PAUL MUNOZ; PRO SE.
- Petitioner

v.

CENTRAL TELEPHONE COMPANY NEVADA; ET AL
-Respondents

On Petition for a Writ of Certiorari to the United States Court of Appeals for the 9th Circuit

APPENDIX U-V-W-X
VOLUME 5

EDDIE PAUL MUNOZ ; Pro Se
P.O. BOX 61344
LAS VEGAS, NEVADA 89160

APPENDIX U

PGS 270- 282

P.U.C. DOCKET.00-6057

BATES RECORD 010420 – 10438

F.C.C. SLAMMING INCIDENTS

TOLL FRAUD EXHIBIT

DOCUMENTED EVENT

INTERSTATE 800 NUMBERS

PREEMPTS FEDERAL JURISDICTION

Slamming Incidents

Trouble tickets incidents of slamming their were 4 incidences of slamming to another carrier MCI the importance of how devastated problem this is that it cuts off your billing which with 800 number. We pay for the usage payphone access etc. with the system that was set up had seventy eight 800 numbers 440-3500 thru 440-3599 100 DID numbers 24 PBX trunks which where supposed to be capability to hotel trunks which Sprint offers to business customers with end to end guarantees of trunking and fibers routes of hotels CEN reference this problem kept occurring this was not just one number we're talking about, 200 numbers that were slammed to the extent of having to put pic freeze on all numbers to keep them from being slammed these problems are very timely to a customer and costly due to lack of business and finding the problem and getting through this process do due to Sprint LD and local Sprint to work together. This stops all calls from coming in.

CEN 108 to 114
CEN 1464 to 1466
CEN 1543 to 1564
MUNOZ 000551-000552
MUNOZ 00304-000303-000296
CEN 1595
CEN 107 to 114
MUNOZ 000548 to 000556
MUNOZ 000560
MUNOZ 000566
MUNOZ 000335-000334
MUNOZ 000331-000326-000314-000307-000298-000297-000271-000270-000269-000268-000267-000266-000265
MUNOZ 000251-000167- to 000172
MUNOZ 000136-000135

Slamming

What you should know about Protecting you telephone service

State of Nevada
Public Utilities Commission

Carson City, Nevada
(775) 687-6000

Division of Consumer
Complaint Resolution

Las Vegas, Nevada
(702 486-2600

This page is best viewed at 800 x 600 resolutions

WHAT IS SLAMMING?

Slamming is the term used when your local or long distance carrier is illegally change without your consent

HOW CAN THIS HAPPEN

There are a number of ways unethical sales people can cause your phone service to be switched without your knowledge. The Federal Communications Commission allows companies to use telemarketing techniques to solicit your business. Telemarketers can cause your phone service to be switched by getting you to say "yes" during a telemarketing call. Also, you can inadvertently agree to switch your carrier by signing a card to enter a sweepstakes. In some circumstances, failure to return a postage-paid card within a certain number of days will trigger an unauthorized change. Sometimes a family member or office associate unknowingly authorizes the change.

HOW DO I KNOW I'VE BEEN SLAMMED?

Read your phone bill carefully each month. Make sure your local and long distance carriers are the ones you have chosen. Be familiar with the various charges and services. Also, you can call 1-700-555-4141 and a recording will tell you which long distance carrier is connected to your line.

If you are slammed, call your local phone company and request Primary Inter-exchange Carrier (PIC) protection on your phone line(s). A PIC freeze prohibits any change in long distance carriers without your express authorization.

Take preventive steps by educating your family and office associates. Only one person should have the authority to change your home or business phone company. Make sure everyone knows what to do if they receive calls regarding telephone service.

THE PUCN WILL HELP

The Public Utilities Commission of Nevada's Division of Consumer Complaint Resolution is here to help. In addition to tracking which companies are using misleading or fraudulent tactics, we can work with your long distance and local carriers to return you to your carrier of choice without any charge. We will work to obtain any refunds you are owed due to higher charges. Call us.
We have offices in Carson City (775) 687-6000; and Las Vegas (702) 486-2600.

DO ANY CONSUMER SAFEGUARDS EXIST?
Both the PUCN and FCC have rules that carriers should follow when soliciting a customer to switch phone companies. The rules say the customer is entitled to receive conformation of his requested switch in writing, by calling an 800 verification number and/or by having an independent third party verify the change. However, these consumer safeguards are increasingly being violated as

carriers compete for new customers in the competitive telecommunications markets.

WHAT IS CRAMMING?

Some companies also try to bill you for other calling services which you did not request. This practice is known as "cramming." The best defense is to listen carefully to sales pitches and closely review monthly bills. Whenever filling out sweepstakes entries, read the fine print.

WHAT ELSE CAN I DO?

You need to be a savvy phone customer. Ask questions. Never allow your service to be changed unless you fully understand the new rates and services you will be receiving. Sometimes there is a charge to switch phone companies. You need to know the amount of the charge and whether you or the new carrier will pay it.

Do not give out your credit card numbers, Social Security number, or other personal information over the phone to an unknown caller. Also, protect your Personal Identification Number (PIN) or any other personal information form an unknown caller.

You can also instruct a telemarketer to be put on the telemarketer's "do not call" list.

FINES/PENALTIES

Phone companies that break the rules and engage in illegal switching are subject to fines up to $100,000 per offense by the Federal Communications Commission. The FCC's toll free number is 1-888-225-5322.

They also can be prohibited from doing any business within Nevada. *If you've been slammed, we need to know.*

1.17.01		PUC	Rick Hackman		Meeting
1.18.01		3-Com	Arron Williams		Phone Call
1.24.01	2:33	Sprint	Doug	Slammed	Call regarding long distance
1.19.01		Amtec k	Tim, Jim	Meeting & Testing	Came to office to do test on phone lines
1.25.01		Sprint	Repair personal Patrick truck 825	Repair	Patrick Cichoshi Sprint Repair Truck liscence c820418 Truck 825 came to warehouse found bridge tap put in 1-400 100 200 count Order 145 Service 134 Transmitter brown and red.
1.25.01		Sprint			
1.26.01		Sprint Repair	Nathan	Slammed	Transferred call to Marty Class 71 Needed to call 800-880-8222 Complex repair long distance of 3 368 numbers
1.26.01		Sprint Compl ex Repair	Faye and Teresa		Given Ticket # WB01263768
1.27.01		Sprint Repair	Clint repair		Numbers were slammed to MCI long distance
1.29.01	2:37	Sprint	Scott		Called to reportrepair on lines and long distance change.
1.29.01		Sprint	Jerry		Slammed by

-					MCI
1.30.01		Sprint	Scott Collins	Phone Call	L.D. Cable, mail, Supervenes on TABS
1.30.01	2:11	OCB	Gayland	Phone Call	Doug 800-767-9406 10-10-333-702 slammed to MCI
1.31.01		OCB	Gayland		Natalin Riki Died
1.31.01	1:21	Sprint	Scott Collins	244-7172	Scott received fax I ask him about other lines going to facilities of t-1 line area
2.1.01	11:54	Sprint	Scott	Fax	Faxed to Scott 244-6497
2.2.01	4:00	Sprint	Scott Collins	Phone Call	Talked to Scott about the ling distance not working on 3 of the lines. He said he would get it fixed.
2.3.01	9:00	OCB	Gayland	Phone Call	Phone call to Gayland regarding what the new Hillsboro's phone girls had to say I.D. a switchman of Sprint robbery tape that goes to Hillsboro Enterprise 5030 Paradise Rd. office.
2.5.01		One Source	Segoria		Called to report Caller ID, *69 and consecutive roll over not working. she

					was out to lunch.
2.5.01	2:45	One Source	Segoria	Returned Phone Call	Stated it should be working needs someone at office to check the numbers
2.5.01	1:50		Kevin Poulsen	202-232-5200	Faxed testing report to 318-1112
2.6.01		Russ	Amtec		Order station win phone
2.6.01		Sprint	Scott Collins		Gave Scott information about (CODY) Rio incident
2.6.01		Sprint	Scott Collins		Lines on 3#s with MCI, Long distance back Kevin Poulsen will call him on security holes of Sprint
2.6.01	11:58	Amtec	Russ		Phone Call
2.6.01	11:00	OCB	Gayland		Phone Call Meeting after 6:30PM
2.6.01		Private Investi gator	Bert Goodrich		Phone Call
2.6.01	12:20		Kevin Poulsen		Phone Call
2.6.01	12:22	Sprint	Scott Collins		Left Message
2.7.01		Private Investi gator	Bert Goodrich	877-9149	Phone Call
2.7.01		Nevad a PUC	Ms Uttinger		Phone Call discussion RE: case 2 hour phone call
2.7.01	12:00	Nevad a PUC	Ms Uttinger		Phone Call
2.7.01	2:50	Attorn ey	Peter Alpert		Mrs. Uttinger called Mr. Alpert

2.7.01	3:00	Private Investi gator	Burt Goodrich		Phone Call
2.7.01			Kevin Poulsen		Left Word
2.7.01	4:03		Bobby Siller		Phone Call
2.7.01		Amtec	Jimmy	909-888-6932	Not until Monday
2.7.01		Nevad a PUC	Ms Uttinger		Fax
2.8.01			Kevin Poulsen		Kevin gave Lois Uttinger phone number
2.10.01			Kevin Poulsen		Phone call Kevin said he talked to PUC
2.10.01		OCB	Gayland		Phone sprint employees
2.10.01		Sprint Repair	Jody	888-862-8293 option 2	reported 368-6494 1-24-01 to Monica would call before noon given trouble ticket 165240
2.11.01	7:21	Sprint	Randy		Took off bridge tap last week
2.11.01	7:27				All lights lite up
2.12.01		Sprint Repair	John Parker and Randy T-one specialist		Ticket number 165240 closed reopen with New Ticket # 165674 T-1 spect switch problem signaling 457-5958 Scott Collins said circuit was nasty had to check transmission and switch. The ticket was closed before calling me.

(pages 2-8)

May-23-01 01:14pm From-BMO
7022444282 T-785 F-698
Datea=20102 User:uum990a 05/23/01

VIEW ALL REMARKS

UNABLE TO DIAL LONG DISTANCE FROM..
01/26/01 20:11 uum8372
LNS: 362-1364, 364-4873, 365-8873 & 367-7831.
GET TRAILOR OF 21H.
CONT. PEGGY OR ED @ 702-368-6494
ACC. 24HRS.
Opened arbs tkt 6224931 and referred to co dspch
01/26/01 22:47 h589221 for ca/pr test*****
THIS SUB HAS BEEN SLAMMED TO MCI. SHOULD
BE SPRINT 01/27/01 18:21 b667869
PLEASE CHG RCDS AND CHG IN SWITCH CHK W/
SUB FOR COMP INFO.
PLEASE CHANGE PIC BACK TO SPRINT, THEY
WILL NEED TO CALL BCAO MON AM TOLD
PEGGY WOULD CALL THE TA & SEE IF THEY CAN
CHANGE IT BACK 01/27/01 18:21 b667869
CALLED ON CALL TA TO CHANGE PIC BACK
Changed all pics to sprint**** 01/27/01 18:48 h589221

NEXT PREV DATE ADD UPDATE TOP BOTTOM
EXIT

May-23-01 01:14pm From-BMO
7022444282 T-785 F-698
Datea=1117 User:uum990a 05/23/01

SERVICE – ALL WORK ORDER DATA

Labor Price:	0.00	Labor Cost:	0.00
Part Price:	0.00	Part Cost:	0.00
Expenses:	0.00	Expense Cost:	0.00
Travel Price:	0.00	Travel Cost:	0.00
Flat Charge:	0.00	Type: Prm. CSR:	h589221
Start Milege:	0.00	Sec. CSR:	
Ending Mileage:	0.00	W.O. Paid?:	
Travel Time:	00.00	Restock Fee: 0.00	COD: no
Job Time:	0000:00	Job Number: Job Phase:	
Bill Time:	0000:00	Invoice: B013111798	
Bill Type:	3	Div: 776	
Customer PO:		Exempt: N	
P.M. Done:	N	Time Zone Number:	3
Tax Code: 290030080		Present Reading:	0.00
W.O. Class:		Last Reading:	0.00
Customer Code: 27781000		Cross Reference W.O.:	
Zip Code:	89119-1226	Territory: T-SOUTNV01	

NEXT-PAGE-Contract Information, PREV-PAGE-Return to the previous screen

SERVICE – ALL WORK ORDER DATA

W.O. Number: WB02274824 Site: 27781001
COMPUTER CONSULTING & DESIGN
Product Ref: Ent By: uuc732e Rem: Y
Serial Number: $2427781001001 Priority: 10 Hold: N
Model Number: ACCESS LINE W.O. Type: R3
Accepted: P
Caller: EDDIE MUNOZ Arr Tech Sup Date:
W.O. Phone: 702-368-6494 Leave Tech Sup Date:
Entry Date: 02/27/01 16:27
Dispatch Date: 02/27/01 16:27
Proj Arr Date: 02/28/01 15:27

Arrival Date: 02/28/01 15:27
Date Completed: 03/01/01 08:52
Cause: u Repair: ref Problem: 38
Subcontractor:
Retrofit:
Current Status: CI
Urgency Code: R
Premise Charge: 0.00
Action Group: wsaved Action Item:

NEXT-PAGE-Additional Information, F12-View Interrupts, F21- View Derts

May-23-01 01:14pm From-BMO
7022444282 T-785 F-698
Datea=20102 User:uum990a 05/23/01

VIEW ALL REMARKS

702-368-6494 AND 362-1366 UNABLE TO DIAL LONG. 02/27/01 18:32 uuc732e E
DISTANCE NUMBER EXAMPLE 775-372-5574. WAS TOLD BY SPRINT LONG DISTANCE TO CALL REPAIR CONTACT EDDIE MUNOZ @ 702-368-6494. ACCESS HOURS 24.
REPAIRED ACCESS LINE REPORTED BY EDDIE MUNOZ D
QUOTED TIME AND MATERIAL CHARGES TO EDDIE MUNOZ 02/27/01 18:33 uuc732e E
STATED HAVE A MAINTENANCE CONTRACT.
Opened arbs tkt 8232320 and referred to co dspch
02/27/01 23.20 h589221 E
for ca/pr test****
arbs ticket closed..ll
03/01/01 10:51 1724161 E
NEXT PREV DATE ADD UPDATE TOP BOTTOM EXIT

Task Name: 5182948
Customer Name: COMPUTER CONSULTING &
DESIGN SD: LNP: P
?Lead Task Nm:
Address: 4372 E. BOSTON AVE.
Phone Number: 702-368-6494
Billing Phone: 702-368-6494 Seq. Num: 0000001
Customer Type: B Circuit Num:
Status: ACT Out of Svc:N Orig OSS: N
Class of Svc: 71 Service Type: POTS
# of Emps: 1 Report Categ: 1
?Skill: AUTO
Sub-Grid: 9N29 Maintenance: N
?Grid: E703
Access Code: Z Ticket Type: Appt Time:
Alarm Set: # of Repeats: 1
Tot Mins: 0 CTT Number:
#of Subseq: 0 Priorty Cd: 3
Due Date: 12/01/00 Due Time: 1845
Ver Code: Orig Due Date: 12/01/00
Orig Due Time: 1845 Test Date:
Log Date: 12/01/00 Log Time: 1101
Test Time: Party Pos: N Dev CD: 1Z
Essen Srv: N Adverse Comm?: Printer:0000
TROUBLE TICKET HISTORY
Lead Employee on this Trouble:
Dispatched To/ Trx Date/Trx Time/ Actual
Estimated
Dispatched-Updated by Duration

Proc	Status	Log Date	Log Time	Duration
PR	ACT	12/01/00	1102	0
0				1

UDS, UDS
Route Date: 12/01/00
PR ACT 11/30/00 1634 0
0
UDS, UDS
Route Date: 11/30/00

APPENDIX V

PGS-A- 283- 288

SECRET SERVICE CORRESPONDENCE

F.C.C. CORRESPONDENCE

SECURITIES EXCHANGE
COMMISSION WASHINGTON D.C.

UNITED STATES POSTAL SERVICE
First-Class Mail
Postage & Fees Paid
USPS Permit No. G-10

(Post Marked:
Las Vegas, NV 89014
23 May)

Sender: Please print your name, address, and ZIP+4 in this box

EDDIE PAUL MUNOZ
P.O. BOX 61344
Las Vegas, NV 89160

SENDER: COMPLETE THIS SECTION

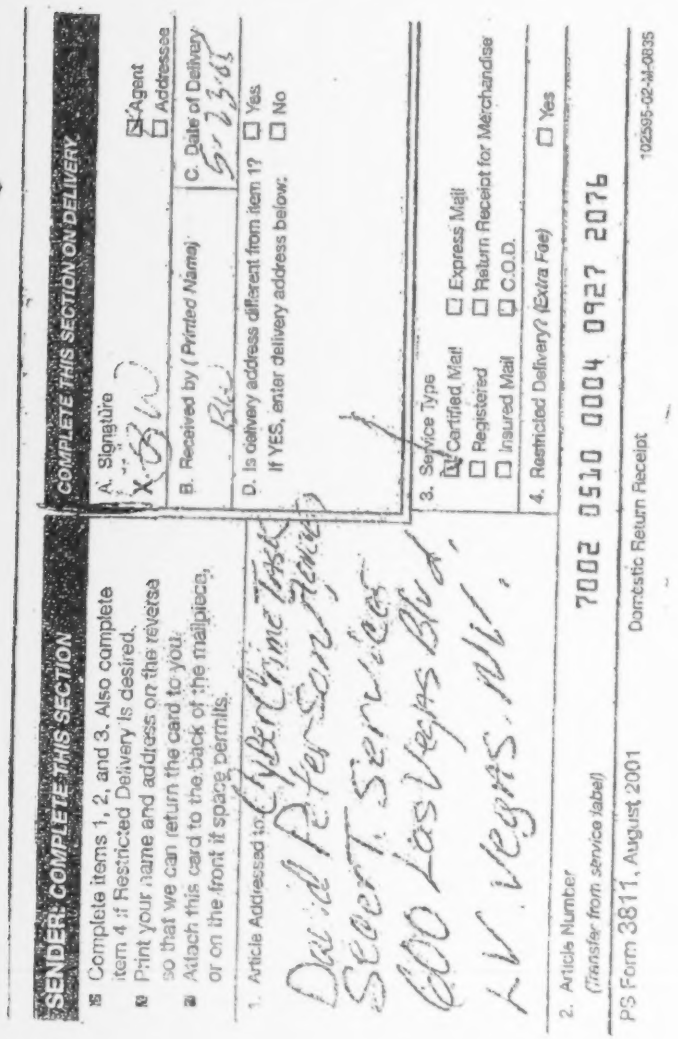
- Complete items 1,2, and 3. Also complete item 4 if Restricted Delivery is desired.
- Print your name address on the reverse so that we can return the card to you.
- Attach this card to the back of the mailpiece, or on the front if space permits.

1. Article Addressed to: Cyber Crime Task Force
   David Peterson
   Secret Service
   600 Las Vegas Blvd.
   Las Vegas, NV
2. Article Number: 7002 0510 0004 0927 2076
   (Transfer from service label)
3. Service Type
   *Certified Mail ☐Express Mail
   ☐Registered
   ☐Return Receipt for Merchandise
   ☐Insured Mail ☐C.O.D.
4. Restricted Delivery? (Extra Fee)

COMPLETE THIS SECTION ON DELIVERY

A. Signature: X (s) *Agent □Addressee
B. Received by (Printed Name): BW
C. Date of Delivery: 5-23-05
D. Is delivery address different from item 1? □ Yes
If YES, enter delivery address below: □ No

PS Form 3811, August 2001 Domestic Return Receipt
102595-02-M-0835



BEST AVAILABLE COPY

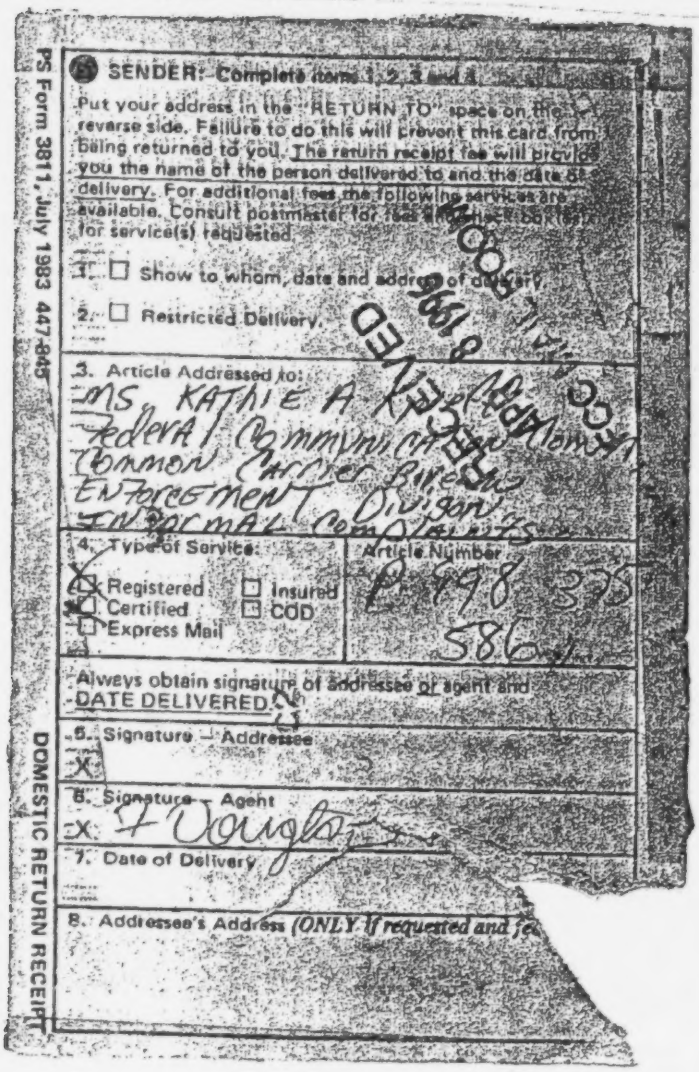
Thank You for your recent telephone inquiry regarding the status of your complaint about telecommunications common carrier service.

[ ] Your complaint File No. IC ____-_____ was received by the Consumer Protection Branch on _____. Pursuant to Section 208 of the Communications Act of 1934, the respondent carrier(s) has/have filed their response(s). The record is now being reviewed to identify possible violations the Communications Act, FCC Rules or Orders.

[ ] Your complaint, File No. IC ___-_____ has been served on the responsible carrier(s), and we are awaiting its/their response(s).

[X] Due to the high volume of complaints, your complaint has not yet been processed by the Consumer Protection Branch.

Thank you for contacting the Consumer Protection Branch.



PS Form 3811, July 1983 447-845

DOMESTIC RETURN RECEIPT

SENDER: Complete items 1, 2, 3 and 4.

Put your address in the "RETURN TO" space on the reverse side. Failure to do this will prevent this card from being returned to you. The return receipt fee will provide you the name of the person delivered to and the date of delivery. For additional fees the following services are available. Consult postmaster for fees and check box(es) for service(s) requested.

1. ☐ Show to whom, date and address of delivery.
2. ☐ Restricted Delivery.

3. Article Addressed to:
MS. KATHIE A KEHOE
Federal Communications
Common Carrier Bureau
Enforcement Division
Informal Complaints

4. Type of Service:
☒ Registered ☐ Insured
☒ Certified ☐ COD
☐ Express Mail

Article Number
P 798 335 586

Always obtain signature of addressee or agent and DATE DELIVERED.

5. Signature – Addressee
X

6. Signature – Agent
X F Douglas

7. Date of Delivery

8. Addressee's Address (ONLY if requested and fe

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
450 Fifth Street, NW
WASHINGTON, D.C. 20549-0213

August 3, 2002

Direct Dial (202) 942-7043
Office Of Investor Education And Assistance
Fax (202) 942-9634
E-Mail: SchockL@sec.gov
www.sec.gov

File No. HO 367907

Eddie Munoz
PO Box 61344
Las Vegas, NV 89160

Dear Mr. Munoz:

Thank you for your comments to the U.S. Securities and Exchange Commission concerning Sprint in Las Vegas. We welcome your comments because they help us to regulate and to enforce the laws that assure fair and orderly securities markets.

I have passed your views on to the people at the SEC who specialize in the issues you have raised. If they have any questions or wish to respond directly to your comments, they will contact you.

Once again, thank you for taking the time to inform us of your views.

Sincerely,
(s)_____
Lori J. Schock
Staff Attorney

APPENDIX W

PGS –A-289- 293

UNITED STATES SENATOR
HARRY REID

U.S. SENATOR
PUBLIC HEARING
APRIL 13 2006
5:30 PM

PUBLIC STATEMENT

SENATOR REQUEST

ENDER: COMPLETE THIS SECTION

Complete items 1, 2, and 3. Also complete item 4 if Restricted Delivery is desired.
Print your name and address on the reverse so that we can return the card to you.
Attach this card to the back of the mailpiece, or on the front if space permits.

Article Addressed to:

Fredo Rid.
FIT, Tom Breda.
333 LV Blvd.
Suite 8016
LV NV 89101,

COMPLETE THIS SECTION ON DELIVERY

A. Signature
X
☐ Agent
☐ Addressee

B. Received by (Printed Name) Luis Zaragoza
C. Date of Delivery

D. Is delivery address different from item 1? ☐ Yes
If YES, enter delivery address below: ☐ No

3. Service Type
☐ Certified Mail ☐ Express Mail
☐ Registered ☐ Return Receipt for Merchandise
☐ Insured Mail ☐ C.O.D.

4. Restricted Delivery? (Extra Fee) ☐ Yes

Article Number (Transfer from service label) 2026 4460 9000 0287 5002

Form 3811, February 2004 Domestic Return Receipt 102595-02-M-1540

United States Senate

WASHINGTON, DC 20510-2803

April 2006

Eddie Munoz
Strip Advertising
PO BOX 61344
Las Vegas, Nevada 89160

Dear Eddie:

I am honored to invite you to join me at an event with the Southern Nevada Chambers o Commerce on Thursday, April 13, 2006 at 5:30 pm. I will be addressing various issue facing the Southern Nevada economy, business community, and workforce. I look forward to hearing from you as a member of commerce on these and other important issues.

The Joint Chambers event will be held at the Clark Count Government Center Pyramid Building at 560 S. Grand Central Parkway in downtown Las Vegas.

Pleas RSVP to Tom Brede in my Las Vegas office as soon as possible by phone (702) 388-5020, fax (702) 388-5030, or e-mail tom_brede@reid.senat.gov. I look forward to seeing you there!

My best wishes to you.

Sincerely,

(s)_____

HARRY REID
United States Senator

STRIP ADVERTISING
P.O. BOX 61344
LAS VEGAS, NEVADA
89160

DEAR SENATOR REID,

HERE'S THE INFORMATION THAT YOU REQUESTED AT THE FORUM FOR THE BUSINESS COMMUNITY OF NEVADANS. IT IS HARD TO UNDERSTAND WHY? PEOPLE HAVE BEEN HIDING THESE ISSUES, FROM ONE OF ARE GREAT LEADERS, I HAVE BEEN FIGHTING THESE ISSUE'S SINCE 1991.
AND FOR ME SPEAKING ON THE TRUTH FOR ARE COMMUNITY AND STATE THE OF NEVADA. MY FAMILY'S BEEN HERE SINCE THE 50'S AND WE CAN'T RUN BACK HOME AND HIDE. FROM INLAND TERRORISTS, THAT ARE TAKING CONTROL OF OUR BUSINESS DAILY WHICH MAKE'S ME MADDER AND MADDER AT PEOPLE .THAT HIDE FROM THESE ISSUES BECAUSE THEY CAN'T STAND UP AND FIGHT FOR WHAT'S RIGHT HERE IN NEVADA. WE ARE AT WAR ,AND THE PEOPLE OF NEVADA NEED TO UNITE AND STAND UP AND BE AMERICAS. I THOUGHT THAT'S WHAT THIS GREAT NATION STOOD FOR, I HAVE LOST EVERYTHING MY FAMILY, MONEY AND INTEGRITY OVER THESE ISSUES THAT STAND BEFORE US. MY LIFE HAS BEEN IN DANGER FOR BRINGING THESE ISSUES TO THE LIGHT OF NEVADAN'S.
NEVADA'S BEEN MY HOME ALL MY LIFE AND AS OUR SENATOR, PLEASE HELP US THE BUSINESSES. NEVADA NEEDS, HELP WE CAN'T GET ANY HELP IN CYBER-CRIME DUE TO ENRON'S POLITICS. NOT WANTING TO ACKNOWLEDGE THAT IT EXISTS DUE TO THE DEPTH OF WAR ON OUR OWN HOME LAND TO

SAVE A BUCK AND PUT OUR CITIZEN'S AT RISK. CYBER-WAR IS HERE AND ARE SYSTEM'S ARE FAILING NEVADAN'S AND OUR BUSINESS'S.

THANK YOU SINCERELY,

EDDIE PAUL MUNOZ
(S)_____

APPENDIX X

PGS-A- 294-339

STATE OF NEVADA OFFICE
OF THE ATTORNEY GENERAL

CYBER CRIME NEVADA TASK FORCE

P.U.C. DOCKET 00-6057
BATES RECORD 010022-010028

DANIEL A MORRIS
ASSISTANT UNITED STATES ATTORNEY

COMPUTER AND TELECOMMUNICATIONS
COORDINATOR

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL

CYBER CRIME

- The Cyber Crime Task Force of Nevada Offers These Tips:
- Fighting Nevada High Technology Crime
- A Strategic Plan To Combat High Technology Crime
- Link to Criminal Justice Statistics Center
- Keeping You Child Safe on the Information Superhighway

For more information on the Cyber Crime Task Force of Nevada, visit their website:

CYBER CRIME
NEVADA TASK FORCE

http://ag.state.nv.us/hi_tech/home.htm 12/20/01

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL

HIGH TECH CRIME IS THE FASTEST GROWING THREAT IN THE AGE OF THE INTERNET – EVERY BUSINESS IS AT RISK. THE ATTORNEY GENERAL AND NEVADA'S HIGH TECH CRIME TASK FORCE OFFER THESE TIPS:

REVIEW SECURITY MEASURES:

1. Inventory and tag all equipment; keep operating manuals, warranties and proof of purchase. Have a reputable security specialist analyze your security procedures. Ask local law enforcement for their advice. If you hire security staff, provide them with adequate training.

2. Adopt written procedures for security and for the use of all high tech equipment including disposal of obsolete or broken equipment. Specify for what purposes the equipment may or may not be used, and whether the company is the owner of all work produced with company equipment.

3. High tech spies target insiders, repair persons, janitors, customers and consultants. Be cautious about divulging security information to others.

EMPLOYEES:

1. Conduct thorough background checks on all new employees, including temporary hires. Include criminal background checks where authorized by statute. Do not allow temporary staff access to sensitive data.

2. Train employees to be careful with sensitive data. Require that all waste documents be shredded.

3. Change passwords and locks when an employee is terminated or otherwise leaves your business.

4. Teach delivery staff techniques for avoiding cargo theft.

COMPUTERS:

1. Require employees to keep passwords confidential; change passwords frequently.

2. Periodic audits of company records should be conducted by a reputable service experienced in auditing computer accounts. Traditional accounting controls should not be abandoned when an office is computerized.

3. Require employees to back up their computers at least once per day. Adopt procedures for making hard copies of computer produced information. Secure backup tapes and diskettes.

4. Take steps to ensure that client information (financial, medical, legal or otherwise) is adequately secured.

5. Ensure that every computer operation can be handled by at least two employees.

6. Maintain adequate surge and anti-virus protection.

7. Remove all data from the hard drive before disposing of your old computer.

THE INTERNET:

1. Check the internet for your own product. This may help you uncover scams or false representations involving your product or service.

2. Don't keep banking or other confidential data on the same computer on which you have internet service.

3. Train employees regarding the hazards of divulging personal or confidential information on the internet.

4. Adopt written procedures for the use of internet services by employees.

TELECOMMUNICATIONS:

1. Establish procedures for the use of long distance service, cell phones, and other telecommunications equipment.

2. Verify the identity of people representing themselves as phone company technicians or repair persons by calling the company itself.

3. Be wary of delivery persons who ask to use your phone. Require that your staff place the call.

4. Train your staff to be on alert for "phone clones" and to report any unusual telephone activity or billings.

IDENTIFICATION:

1.Train employees to check credit card numbers and to compare information on the face of a credit card with the information printed out on the receipt.

2. Businesses which employ drivers should be alert for false drivers licenses and auto insurance certificates.

3. Develop a system for marketing or coding purchase orders, checks and other documents involving the financial transactions of your business so you will know of they are yours or are counterfeits.

4. Require fingerprints from customers presenting checks, money orders or traveler's checks.

GENERAL TIPS:

1. Be alert for suspicious behavior, such as the unexplained presence of persons in unauthorized areas.

2. If you observe anyone rummaging through garbage for papers, notify local law enforcement.

3. Adopt a "zero tolerance" approach toward high tech criminals. Prevent crime as best you can, but when it is detected, insist on pressing criminal charges and pursue all available civil remedies.

4. Knowing how your company's high tech equipment works will help you understand how to protect your business. Take any training which is offered at the time you purchase high tech equipment, read the manuals and get some "hands-on" experience with the new product.

5. Take any training which is offered at the time you purchase high tech equipment, read the manuals and get some "hands-on" experience with the new product.

A Message From Frankie Sue Del Papa

"Protecting your business from high tech crime does not have to be expensive or time consuming. The Office of the Attorney General and that University of Nevada Small Business Development Center have offered seminars to help small businesses learn from experts, and to teach law enforcement how to better prevent high tech criminals from stealing equipment, sabotaging or stealing customer and client information, charging long distance calls to business accounts, and using counterfeit checks and false identification to obtain products and services. Senate Bill 485 of the legislative session created the High Technology Crime Advisory Board which will be responsible for continuing the education of the business community and the general public."
If you are interested in assisting the Nevada High Technology Crime Task Force, a group of representatives from law enforcement and the business community working together to fight high tech crime, contact the Attorney General's Office (Kevin Higgins at 688-1818). Your suggestions, comments and ideas are welcome.

5/01
HIGH TECH CRIME
TIPS FOR BUSINESSES TO FIGHT HIGH TECH CRIME
NEVADA HIGH TECHNOLOGY CRIME TASK FORCE
OFFICE OF THE ATTORNEY GENERAL
Frankie Sue Del Papa Attorney General
100 N. Carson Street
Carson City, Nevada 89701-4717
(775) 687-4170

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

A Strategic Plan To Combat High Technology Crime In Nevada

CONTENTS

- Task Force Recommendations
- Executive Summary
- Members of Nevada's High Technology Crime Task Force
- Steering Committee Members
- Introduction
- Crimes Involving Computers and Components
- Computer Intrusion
- Telecommunications Fraud
- Technical Forensic Expertise and Assistance
- Prosecution Assistance

...to assist with the national endeavor against computer criminals. Efforts are also underway to enlist members of our country's computer industry to assist us in this fight and we are working towards getting a panel on this subject on the agenda for next year's COMDEX Convention in Las Vegas.

There are different ways you can help us in these efforts. If you or other members of your business can contribute expertise or equipment that would be of use to the task force, please contact Anne Cathcart of the Attorney General's Office at: (702) 687-3541.

The Task Force, in cooperation with the University of Nevada system, has planned a series of training seminars for businesses. These will be held beginning in February. For further information on participating in these seminars, please contact Kathy Carrico, State Training Director at the University of Nevada, Reno, at: (702) 784-1717.

The Attorney General's Office and the High Technology Task Force have developed a brochure with tips for businesses to help them combat high technology crimes. A copy of that brochure is included.

The involvement of the business community was identified by the task force as essential in helping to better equip law enforcement in their efforts to protect the community as a whole. Your suggestions, comments or ideas are needed, indeed, your participation is vital. Together, we can coordinate and share our resources to better fight the criminal elements in this new age of cyber crime.

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

EXECUTIVE SUMMARY OF TASK FORCE FINDINGS

Crimes involving computers and other high technology crime are the fastest growing criminal movement in the country. Computer crimes cost private industry between $5 billion and $10 billion annually. This number is expected to rise to $200 billion by the year 2000. Over $1 trillion is transferred every week by electronic wire. In the last five years technology theft has increased 323%. Only 1% of computer crime is being detected and only 7% of the detected crimes re reported to law enforcement. Of the cases which are detected and prosecuted, only 3% result in a jail sentence. Theft of long distance service is estimated at $3.7 billion a year. The average bank robber nets $2500, the average bank fraud nets $25,000 – the average computer crime nets $500,000 and the average theft of technology loss is $1.9 million.

Nevada's number one industry, gaming is a high tech industry which has and will continue to be a target for high technology crime. Cheating techniques often involve the use of high tech equipment and computer software, and may originate outside the state of Nevada.

Crimes are perpetrated against high technology manufacturers, retailers, businesses and homes containing computers and other equipment, and against anyone who makes cellular phone calls or who uses a credit card are common. High tech criminals forcibly take over warehouses and other businesses to steal computer equipment, hijack trucks, steal proprietary business information, perpetrate subscription fraud, cloning and toll

fraud against telecommunications companies and their customers, intrude into and disrupt corporate and government computers, pirate software, create false identification, counterfeit checks and other negotiable instruments and many other crimes. These crimes are committed against high tech targets or use high tech targets or use high tech means, or both.

The Nevada High Technology Crime Task Force was organized in July, 1997 at the direction of Attorney General Frankie Sue Del Papa and is compromised of representative of state, local and federal law enforcement agencies and private industry. The task force was created for the purpose of forming high technology crime units to conduct multi-jurisdictional investigations; track and disrupt the illicit commerce in stolen high tech goods, investigate and prosecute suspects engaged in white collar crime, organized crime and fraud against the government and private industry. The major goals of the task force are to:

- Investigate crimes involving computers and computer components, such as…

http://ag.state.nv.us/hi_tech/executive.htm 12/20/01

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

NEVADA HIGH TECHNOLOGY CRIME TASK FORCE RECOMMENDATIONS

The explosion of high tech crime, the loss of millions of dollars by industry and private citizens, and the danger to society as a whole posed by the high tech criminal mandate a response from law enforcement. The task force strongly recommends the immediate formation of high tech crime units and appropriate training for officers, prosecutors and judges. The task force makes the following specific recommendations:

- FORMATION OF TWO HIGH TECH CRIME UNITS, ONE IN NORTHERN NEVADA AND ONE IN CLARK COUNTY
- MANDATE AND PROVIDE HIGH TECH CRIME TRAINING FOR ALL NEVADA PEACE OFFICERS
- CERTIFY NEVADA LAW ENFORCEMENT OFFICERS IN COMPUTER FORENSIC ANALYSIS AND ASSIGN OFFICERS TO HIGH TECH CRIME UNITS
- EXECUTE MEMORANDA OF UNDERSTANDING BETWEEN ALL AGENCIES PARTICIPATING IN HIGH TECH CRIME UNITS
- PROVIDE BUSINESSES AND CITIZENS WITH EDUCATION IN PROTECTION AGAINST HIGH TECH TECH CRIME
- OBTAIN CONTINUED FUNDING AND SUPPORT FOR HIGH TECH CRIME UNITS

- NEVADA PARTICIPATION IN A WESTERN REGIONAL HIGH TECH CRIMES TASK FORCE
- PROVIDE HIGH TECH CRIME TRAINING TO PROSECUTORS AND JUDGES
- ENHANCE NEVADA LAWS RELATING TO HIGH TECH CRIME
- ESTABLISH STATEWIDE HIGH TECH CRIME DATABASE

http://ag.state.nv.us/hi_tech/recomend.htm 12/20/01

http://ag.state.nv.us/hi_tech/recommend.htm 12/20/01

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

MEMBERS OF NEVADA'S HIGH TECHNOLOGY CRIME TASK FORCE

(The following names were highlighted, taken from a much larger list)

Frankie Sue Del Papa, Attorney General
Alan Gallaspy, L.V. Metro
Steve Gibson, Esq., Lionel Sawyer & Collins
Kevin Higgins, Sr. DAG, A.G.'s Office
David Peterson, L.V. Metro
Bob Swiatek, Chief Inv., A.G.'s Office
David Vansant, FBI
Michael Taylor, Storey Co.
David Thompson, DAG, A.G.'s Office

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

STEERING COMMITTEE MEMBERSHIP

(The following names were highlighted, taken from a much larger list)

Lou Emmert, Sprint
Steve Franks, LVMPD
Jerry Kellar, Sheriff Clark County

State of Nevada -- Attorney General/Hi-Tech Crime/Plan 2

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

2. CRIMES INVOLVING COMPUTERS AND COMPONENTS.

Employee theft from manufacturers. When computer chips and components worth thousands of dollars can easily be hidden in an employee's pocket, some people cannot resist the opportunity to unjustly enrich themselves. These components are often untraceable and easily sold on the 'gray market' to less than honest manufacturers and retailers. We go to great lengths in the casino and mining industries in Nevada to prevent crimes of opportunity by employees, but is the same attention paid to the problem in our high tech industries? Such crimes should be prosecuted based on the value of the property stolen, which is oftentimes in the range of a major bank robbery. While employee theft is usually non-violent, it should not be relegated to the slap on the wrist associated with other white collar crimes.

Theft from computers at non-high tech businesses and institutions. The PC on a desk has become common place, but little though is given to securing this equipment from theft. But when an individual workstation and printer can be worth thousands, and the equipment in even a small office tens of thousands, businesses and public agencies become a preferred target for the high tech criminal. Most businesses and agencies have minimal after hours security, and simply by jimmying a door or breaking a window on late weekend night, a burglar can hit the jackpot. A retail store with an equal amount of inventory usually secures its goods at night, has an alarm system and is periodically checked by a security service. Most of

us unthinkingly leave essentials and extremely expensive equipment in an office in plain view from the street.

Fraud, counterfeiting and piracy. One of the biggest problems facing law enforcement is that many crimes are not even thought of as crimes by those who commit them. Does the average computer user think of copying someone else's software in the same way he thinks of shoplifting or petty theft? How many local businesses have proof of ownership for ever piece of software they are running? Microsoft recently sued several small computer manufacturers in the Bay Area for installing thousands of pirated copies of Windows on the PCs they sold. Failure to enforce the laws against software piracy only adds t5o the culture that creates users who do not think breaking into a computer system is a crime either. Another serious problem for the high tech industry is the counterfeiting of high tech products, including fake labels and equipment identification, and re-routing equipment by changing shipping labels.

Related crimes. The experience of the Sacramento Valley High Tech Crime Task Force is that the people and gangs involved in these new high tech crimes are also involved in many traditional crimes. Raids on high tech criminals have turned up piled of stolen and cloned cell phones as well as quantities of controlled substances and weapons. These new criminals seem to be following the business plan of the 90's and are diversifying their operations, incorporating high technology to assist them in carrying out traditional criminal activity with the added benefits of anonymity, no physical contact, and no significant financial investment.

Burglary and robbery at manufacturing sites, storage facilities and retail stores. Willie Sutton once said that the reason he robbed banks was because that's where the money was. The millions of dollars of components and equipment held by some computer manufacturers and other businesses has proven to be an irresistible target for

daylight invasion robberies by organized gangs. These robberies are often extremely violent and have resulted in the deaths of employees and bystanders. The proceeds can often be contained in a shoebox and are virtually untraceable. The same gangs are often implicated in telecommunications fraud, extortion, and drug sales and manufacturing. But their most profitable area is high tech theft, which is sure to be a growth industry in the next decade.

Cargo theft. High tech criminals employ various methods of hijacking expensive high tech cargo, especially that which is transported by trucking companies. One method, for example, is for one car to stop in front of the truck and another car drop directly behind the truck, making it impossible for the truck to go forward or backward. The car drivers then approach the truck driver with weapons. Truck drivers, including those employed by pickup and delivery services, are particularly vulnerable to being placed in physical danger in high tech cargo theft. The task force recommends that ruling companies provide instruction for their employees, to alert them to the various techniques of high-tech criminals. Procedures should also be established by trucking companies and associations to educate truck drivers so they can better protect themselves in at-risk situations.

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

3. COMPUTER INTRUSION.

In the movie War Games a teenage hacker brought the world to the brink of nuclear war. Today stories of hackers and the damage they cause are commonplace. Hackers break into business, private, and government computers to commit fraud, to destroy and alter records, and to simply create havoc. Hackers constantly change their methods and targets both to keep up with the changes in the high tech industry and to avoid detection. Businesses are sometimes blackmailed by hackers threatening to crash companies' file server, delete customer lists and customer e-mail, and corrupt databases.

While the specter of the teenager obsessed with computers working alone in his room at night is often the first image that comes to mind when thinking of computer intrusion, the more likely suspects are insiders, commonly greedy employees, or disgruntled former employees seeking vengeance. Who better knows how to break into your system and access sensitive information then the person who designed worked with it daily?

There are many basic measures a business can include in its procedures, such as changing passwords when an employee leaves, limiting access to high-level network functions, arranging for periodic audits, shredding its paper garbage, and many other steps, which can limit the possibility of crimes of opportunity.

One of the challenges facing the task force is that few businesses that are victims of computer intrusion report the crimes to law enforcement. Oftentimes there is a great

reluctance to let ones' customers, competitors o members of public know that the company's security has been compromised. May businesses would seem to prefer to absorb the loss in silence rather than risking the publicity which might accompany a prosecution. Unfortunately, this posture only serves to encourage high tech criminals.

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

4. TELECOMMUNICATIONS FRAUD

From the cloning of cell phones to the theft of calling cards to the slamming of long distance services, the average American is now the potential victim of a myriad of crimes that did not exist 20, 10 or even 5 years ago.

How do we begin to protect our citizens from crimes that can be committed without the criminal ever meting the victim face to face? The traditional law enforcement practice of having the victim or witnesses identify the perpetrator in front of a jury does not work for crimes committed by remote control.

By far the easiest way to deal with telecommunications fraud is to prevent it from happening. Deterrence is also a key element, but that works only of the criminal knows that similar cases have resulted in swift prosecutions and severe punishment.

Communications companies have begun to develop the ability to detect or prevent some types of criminal activity in the telecommunications area. For example, AT&T can disconnect cloned calls before the call is connected, because each phone has its own "fingerprint" which can be identified immediately upon placement of the call. AT&T's success with this phone print service has resulted in fewer phone cloning instances, but the service is not inexpensive.

Probably the most effective way to reduce telecommunications fraud is through the education of the public. Alerting users about the methods by which high

tech criminals attempt telecommunications fraud is essential for reducing such crimes as phone service subscription fraud. Both the telecommunications industry and the consumer must cooperate in the prevention and detection of these types of crimes.

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

5. TECHNICAL FORENSIC EXPERTISE AND ASSISTANCE

The investigation and prosecution of high tech crime present a special challenge to law enforcement. Law enforcement has fallen far behind the high tech criminal. Law enforcement officers have to learn such basic matters as what the primary components of a computer look like, how to secure the scene at computer crime (without inadvertently destroying evidence), how to handle high tech items and how to prevent suspects from erasing evidence right in front of them. Every line officer must be trained to recognize high tech equipment such as microprocessors, SIMMs, CD ROMs, mother boards, cloning devices and other evidence of high tech crime such as forged IDs and negotiable instruments. In the absence of this type of basic training, law enforcement will remain unable to respond effectively to high tech crime.

Officers must also be trained in the highly technical forensic analysis of computer software and hard drives. Officers must also understand the sophisticated technology used to commit high tech crime and must be certified computer forensic examiners in order to present evidence effectively in court.

This type of criminal activity is particularly complex and an officer handling computer crime needs a much lower caseload than other officers. It must also be noted that in order for a law enforcement agency to address high tech crime, officers must be dedicated full time.

The investigative complexity of these crimes requires painstaking and time-consuming analysis of crime scenes and seized evidence, and the creation of comprehensive profiles of high tech criminals. Establishing high tech forensic labs and databases is essential. It is a goal of the task force to assist Nevada law enforcement in overcoming these obstacles.

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

6. PROSECUTION ASSISTANCE.

Prosecutors and judges are similarly lacking in expertise and understanding of the technology utilized by the high tech criminal. High tech crime case law, although slowly evolving, is sparse and in many areas non-existent. The task force intends to provide ways to assist prosecutors and our courts in dealing with the high tech criminal.

In order to be able to present a high technology crime case to a jury, the prosecutor and the judge must have a fundamental understanding of the technical issues involved before they can hope explain them to someone else. By sponsoring training programs directed specifically at judges and prosecutors the task force can create a cadre of computer literate people who are ready to handle these complex cases.

It is recommended that programs for judges and lawyers be developed with the assistance of the National Judicial College, the Nevada Bar Association (Continuing Legal Education), the Nevada District Attorneys Association, and the newly formed Prosecution Advisory Council. The curriculum should include instruction on the preparation of lawful search warrants when high tech crime is involved; preservation of the evidence and establishing the chain of custody; qualifying and questioning expert witnesses in computer forensics; privacy and First Amendment issues; jury instructions in high tech crime cases; and the use of high tech demonstrative evidence.

Just as the task force recommends the dedication of law enforcement officers who receive training and acquire adequate experience to handle search and seizure situations, investigation techniques, and arrest in the high tech crime, the task force similarly recommends that there be at least one full-time prosecutor with training and experience in prosecuting high tech crime cases for each of the high tech crime units established in the state, one in the Las Vegas unit and one in the Reno/Sparks/Carson City area unit.

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

8. BUSINESS AND PUBLIC EDUCATION

Both private industry and the general public must be educated about high tech crime in order to defend against it. Simple techniques can be used to restrict access to computers and to prevent other intrusions (password changing, turning equipment off, maintaining confidentiality of social security numbers and other personal information). Businesses and individual's can be trained to identify pirated, cloned and stolen goods and to recognize forged instruments.

Private industry should also be familiar with high tech crime units and personnel, and be able to obtain appropriate assistance when needed. Many corporations offer toll-free numbers so consumers may check whether a specific piece of equipment was manufactured by the company, and if so, whether it has been reported as stolen. The establishment of two specific high tech crime units in northern and southern Nevada will make it easier for consumers and businesses to report suspected crimes.

A goal of the task force is to provide information to businesses and the general public, and to make training about high tech crime available. The task force is already working with the Small Business Development staff at the University of Nevada, Reno, on a series of seminars which will help owners and managers of small businesses in the community learn how to detect and prevent high tech crime. The task force intends to present similar seminars in southern Nevada. Law enforcement is assisting with similar educational efforts in Las Vegas. Requiring fingerprints on checks, conducting periodic audits of

internal functions, shredding paper documents, and thoroughly checking the references and background of job applicants- including temporary hires- are examples of measures that can be taken to reduce the potential for becoming a victim of high tech crime.

It is important to educate parents about criminal activity on the Internet, which could affect their children, including pornography and pedophilia. Teachers of computer science should be encouraged to include as part of their curriculum discussions on ethics and the law as they relate to high tech use. All Internet customers and especially vulnerable groups such as children, seniors, invalids, and the unsophisticated should be warned of consumer fraud activities on the Internet. Public education would include simple measures as changing the PIN number on a home answering machine; adequately checking on the legitimacy of any business advertising a product or business over the internet; refusing to be coerced into paying certain charges (usually by credit card) when you have been told you have "won" a prize or vacation; being aware of the potential dangers posed by "chat rooms", exercising caution about disseminating or discarding confidential personal data, etc.

The task force members recommend that a strong, cooperative effort to educate the public about high tech crime and its prevention should be initiated. In addition to seminars for business owners and managers, presentations can be made to parent groups and to students of all educational levels. Both corporate representatives and law enforcement officials a join in making public services announcements on television and radio. Brochures and other informational materials, including audio and visual aids, can be developed.

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

9. LEGISLATIVE CHANGES

As part of the effort to combat high tech crime, our laws must be strengthened. The task force recommends the following changes to the Nevada Revised Statutes be considered:

1. Impose stronger criminal penalties for high tech criminals, aiders and abettors, including restitution;

2. Allow businesses to obtain criminal background checks on prospective employees who will responsible for handling confidential data and financial data;

3. Expand definitions of high tech criminal activity to encompass newer forms of technology, which are developed;

4. Enhance ability of law enforcement to obtain search warrants in situations involving suspected high tech criminal activity;

5. Provide adequate resources for law enforcement to establish two high tech crime units in Nevada, including manpower, equipment and training;

6. Provide for strong civil penalties for high tech criminals, which will encourage victims of high tech crime to pursue civil remedies.

7. Work with other states to develop an interstate agreement, which can be enacted by all state legislatures to help eliminate jurisdictional problems.

Copies of current Nevada law related to computer and other high tech crimes are attached in Appendix A.

State of Nevada – Attorney General/Hi-Tech Crime/Plan 10

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

10. HIGH TECH CRIME UNITS/REGIONAL TASK FORCE

High tech crime units must be formed north and south in order to combat high tech crime. Without these units, law enforcement in Nevada will never effectively address high tech crime and will be powerless to respond to the multitude of criminal activity associated with high tech crime. The formation of these units is the primary and most important recommendation of the task force.

Task force members unanimously agree that the only way to combat high tech crime is through a coordinated multi-agency task force approach similar to the Sacramento High Tech Crimes Task Force. The Sacramento Task Force consists of twelve state, local and federal agencies with dedicated personnel and resources administered by the Sacramento County Sheriffs Office. The Sacramento Task Force has seven investigators who work high tech crimes on a full time basis. Other investigators participate part time on one to two shifts per week. The task force was created with the assistance of five comp0uter manufacturers and two cellular companies. Supporting businesses also provided furniture, office equipment, safety equipment, cash for informant fees, training and miscellaneous expenses The Sacramento Task Force works closely with the security departments of private companies, and cases are often directly forwarded from company6 security investigators to the task force.

In 1996 the Sacramento Task Force investigates property loss of more than $14 million and recovered more than $9 million. 156 suspects were arrested for illicit commerce in

components, burglaries, on line crimes, telecommunications fraud, financial fraud, gambling, robberies, narcotics and other offenses.
The task force recommends that two high tech crime units be formed in Nevada. One located in northern Nevada to provide assistance locally and to the rural counties, and one located in Clark County. The Office of the Attorney General will serve as a coordinating agency for the initiative against high tech crime and will also continue to provide prosecution assistance to the local entities as needed.

It is recommended that at a minimum, the following local, state and federal agencies should actively participate in the high tech crime units:

Northern Unit

Washoe County Sheriff
Washoe County District Attorney

Reno Police Department
Sparks Police Department
Nevada Attorney General
Nevada Division of Investigation
United States Attorney
FBI
Secret Service
US Postal Service

Southern Unit

Las Vegas Metropolitan Police
Clark County District Attorney
Las Vegas Police Department
Henderson Police Department
Nevada Attorney General
Nevada Division of Investigation
United States Attorney
FBI
Secret Service
US Postal Service

Corporate sponsors should also actively participate in the task force units.

In addition, the establishment of a Western States Regional High Tech Crime Task Force has been proposed to enable western states to enhance their efforts to combat high tech crime. Such a regional group could address issues concerning the multiple jurisdictional questions which arise in high tech crime; recommend legislation which will assist all affected law enforcement in the investigation and prosecution of high tech crimes; facilitate the consolidation and sharing of high tech resources among the western states; provide or coordinate

continuous opportunities for training which are cost-effective; and encourage and develop methods for law enforcement to share information regarding high tech criminal activity. The task force supports the concept of a regional entity.

Tracking a Computer Hacker

Daniel A. Morris
Assistant United States Attorney
Computer and Telecommunications Coordinator
District of Nebraska

A report written near the start of the Information Age warned that America's computers were at risk from hackers. It said that computers that "control [our] power delivery, communications, aviation and financial services [and] store vital information, from medical records to business plans, to criminal records, "were vulnerable from many sources, including deliberate attack. "The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb. "National Research Council, "Computers at Risk, "1991.

To see what computer hackers are doing today, look at www.attrition.org. This is one of the places on the Internet where hackers receive "credit" for their attacks. If the operator of this website verifies that a computer system has been invaded, a "mirror" of the damage, often a defaced web page, is posted on the website along with a link to the undamaged website. More importantly to the person or group claiming credit, the online nickname of the responsible hacker (HaXoBuGz, data boy and HACKWEISER being examples) is included next to the published description o the intrusion. This fleeting notoriety is what motivates many hackers. Other hackers cause even greater damage and try to avoid notice, much less notoriety.

Information about some of the Department of Justice's successes in prosecuting hackers can be found on the Department's website at www.cybercrime.gov. This site includes manuals for searching and seizing computers, policy statements, useful background material, and press releases regarding hacker prosecutions. It is one of the

first places prosecutors should go when called upon to assist investigators looking into computer intrusions.

Hacker Tools Available Online

Some websites on the Internet provide both novice and expert computer hackers with programs, sometimes called "exploits," needed to conduct attacks. These sites may provide services to computer security experts and eve advise hackers that they should not use the posted exploits to hack into another computer. Anybody, including some very destructive people, can download the hacker tools or "scripts" coded by experienced hackers, along with instructions for their use. See, e.g., http://www.securityfocus.com and its "bugtraq" service

Hackers who find exploits on these websites may use them to do more than just deface webpage's. Novices, sometimes referred to in hacker circles as "script-kiddies, "who download hacker scripts may gain "root" access to a computer system, giving them the same power over a computer system as a trusted systems manager – such as the power to create or delete files and e- mails and to modify security features.

Hackers who gain such unauthorized root access sometimes speak of this as "owning" the system they hack. If they want to cause damage they may do so immediately, or they may plant viruses or time bombs in a system. Sometimes they configure the system to work for them in later "denial of services: attacks on other computers.

Some websites that post hacker tools also post known fixes, or patches. They advise systems administrators and network operators to download and install these patches so their systems will no longer be vulnerable to the listed attacks. But hackers know that, with persistence and help from other readily available computer programs, they can find computer systems vulnerable to the listed exploits. Hackers frequently launch their attacks against these unprotected systems.

It is commonly believed that many systems operators do not share information when they are victimized by hackers. They don't contact law enforcement officers when their computer systems are invaded, preferring instead to fix the damage and take action to keep hackers from gaining access again—with as little public attention as possible.

Protected Computers

Federal law enforcement officers may be called in to track a hacker if the hacker gains unauthorized access to a Federal Government computer or to a computer system

protected by federal law. Protected computers are any computer used in interstate or foreign commerce or communications, which includes any computerco0nnecxted to the Internet. 18 U.S.C. & 1030 (e)(2)(B).

Tracking a hacker may call for a combination of Internet research skills, subpoenas, court orders, search warrants, electronic surveillance and traditional investigative techniques. At least one Assistant United States Attorney (AUSA) in every district has been trained as a Computer and Telecommunications Coordinator (CTC) to assist law enforcement officers and other AUSAs in this effort. CTCs can obtain guidance from attorneys in the Department of Justice's Computer Crimes and Intellectual Property Section (CCIPS) (pronounced See-sips). CCIPS attorneys deal with these issues daily.

Clues of a Cyber crime

A clue to the identity of a hacker often exist in cyberspace and in the real world of the investigator knows where to look.

Computer systems of interest to hackers usually keep track of all authorized and unauthorized access attempts. Records, called computer logs, provide useful and often critical clues that a trained agent or computer specialist can use as the starting point to trace the route taken from computer to computer through the worldwide web, to discover the one computer out of the millions in the world from which and intrusion was conducted.

All computers using the Internet are assigned a different numeric Internet Protocol (IP) address while online, similar to country, city, street, and number addresses for houses.
Unless the hacker alters the victim's logs once he or she gains unauthorized access, the victim'[s logs should list the precise computer address from which unauthorized

access was gained. That address may not be the hacker's own computer, but instead another computer that the hacker has hijacked or an account that he owns on a third party's computer, as discussed in more detail below.

Lookup tools are available online to identify the owner of the network through which an attack was launched. To see how this works, see www.arin.net. Operated by the American Registry of Internet Numbers.

Obstacles to Identifying the Hacker

Because of the make-up of the Internet, it is sometimes difficult for law enforcement officers to discover the identity of a hacker.

1. A hacker might hide or "spoof" his Internet Protocol (IP) address, or might intentionally bounce his communications through many intermediate computers scattered throughout the world before arriving at a target computer. The investigator must then identify all the bounce points to find the location of the hacker, but usually can only trace the hacker back one bounce point at a time. Subpoenas and court orders to each bounce point may be necessary to identify the hacker.

2. Some victims don't keep logs or don't discover a hacker's activities until it is too late to obtain records from the hacker's Internet Service Provider (ISP). A victim who has no record of the IP address of the computer from which unauthorized access was gained limits law enforcement officers to traditional investigative techniques, which alone may be inadequate to identify the hacker.

3. Some victims don't keep records or don't keep them long enough to be of help to law enforcement officers. As explained below, when the investigator determines the identity if an ISP from which records will be needed, the prosecutor should send a retention letter under 18 U.S.C.

& 2703 (f) requesting the ISP to preserve the records while a court order or other process is being obtained.

4. Some computer hackers alter the logs upon gaining unauthorized access, thereby hiding the evidence of their crimes.

5. Some leads go through foreign countries, not all of which consider hacking a crime. Treaties, conventions, and agreements are in place with some countries, and there are "24/7" contacts in dozens of countries around the world who can be contacted for help. When a lead points to a foreign country, the investigator should contact a CTC or CCIPS attorney.

Electronic Communications Privacy Act

Some of the information investigators need to track a hacker might be readily available to the general public on the Internet. No special restrictions apply to an investigator's access to and use of such information – in the same way that information available in a public library can be used by investigators without special authorization. Common search engines such as www.dogpile.com www.lycos.com www.excite.com or www.netscape.com may be used to find information about a username or nickname of the person or group claiming credit for a computer intrusion.

Other information, such as the content of e-mails, is available to law enforcement officers only if they comply with the provisions of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. && 2701-11. ECPA creates statutory rights for customers and subscribers of computer network service providers. The details of this Act are beyond the scope of this article, but an excellent guide to the Act is provided by CCIPS in print and on its webpage. See Computer Crime and Intellectual Property Section, Department of Justice, Prosecuting Intellectual Property Crimes Manual.

Section 2703 of ECPA provides investigators with five mechanisms for compelling an Internet Service Provider to disclose information that might be useful in an investigation of a hacker.

The mechanisms, in ascending order of the threshold showing required, are described below:

1. Subpoenas can be used by an investigator to obtain basic subscriber information from an Internet Service Provider, including "the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber or customer utilized. "U.S.C. & 2703(1)(C).

2. Subpoenas also can be used to obtain opened e-mails, but only under certain conditions relating to notice to the subscriber. See 18 U.S.C. & 2703(b)(1)(B). Notice may be delayed under Section 2705 for successive 90-day periods. Subpoenas may be issued for e-mails that have been opened, but a search warrant is generally needed for unopened e-mails.

3. Court orders under 18 U.S.C. & 2703(d) can be obtained by investigators for account logs and transactional records. Such orders are available if he agent can provide "articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an on going criminal investigation." Id.

The government must offer facts, rather than conclusory statements, in an application for a 2703 (d) order. A one to three-page factual summary usually is sufficient for this purpose. The standard for issuing such an order is not as high as for a search warrant.

4. Investigators who obtain a court order under 18 U.S.C. § 2703 (d) can obtain the full contents of a subscriber's account (except for unopened e-mail stored with an ISP for 180 days or less and voice-mail), if the order complies with a notice provision in the statute. 18 U.S.C. § 2703 (b)(1)(B)(ii) and (b)(2). Notice to the subscriber can be delayed for up to ninety days when notice would seriously jeopardize the investigation. 18 U.S.C. § 2705(a).

5. Search warrants obtained under rule 41 of the Federal Rules of Criminal Procedure or an equivalent state warrant can be used to obtain the full contents of an account, except for voice-mail in electronic storage (which requires a Title III order). The ECPA does not require notification to the subscriber when the government obtains information from a provider using a search warrant.

Warrants for information regarding evidence of a computer intrusion are usually obtained like all other search warrants but are served like subpoenas. That is, the agents serving the warrants on an ISP ordinarily do not search through the providers computers. Instead, they serve the warrants on the provider and the provider produces the material described in it.

Voluntary Disclosures

Investigators can obtain the contents of a hacker's communications stored on the victim system without first obtaining an order or a subpoena, pursuant to 18 U.S.C. § 2702(b). For example, a hacker's victim may voluntarily disclose the contents of internal e-mails relevant to the attack.

Voluntary disclosure by a provider whose services are available to the public is forbidden unless certain exceptions apply. These exceptions include disclosures "incident to the rendition of the service or the protection of the rights of property of the provider of the service or the protection of the rights of property of the provider of

the service." 18 U.S.C. § 2702(b)(5). See 18 U.S.C. §§ 2702 (b)(1)-(4), (6)(A)-(B) for other exceptions.

Early Communication with ISPs

Investigators should contact a network service provider as soon as possible to request that the ISP retain records that may be relevant to an investigation. This is often done through the AUSA who is assisting the agent in the investigation. The AUSA should send a letter to the ISP directing it to freeze stored records, communications, and other evidence pending the issuance of a court order or other process. 18 U.S.C. 2703 (f).

If the investigator wants to be sure the ISP does not disclose that the ISP has been asked for information pursuant to a subpoena, order or warrant, an order not to disclose can be obtained under 18 U.S.C. § 2705 (b).

Electronic Surveillance

Investigators tracking down hackers often want to monitor a hacker as he breaks into a victim's computer system. The two basic statues governing real-time electronic surveillance in other federal criminal investigations also apply in this context.

The first is the wire tap statute, 18 U.S.C. §§ 2510-22, generally known as a Title III order. The second statute relates to pen registers and trap and trace devices. 18 U.S.C. §§ 3121-27.

DOJ's manual for obtaining evidence of this type, says "In general, the Pen/Trap statute regulates the collection of addressing information for wire and electronic communications. Title III regulates the collection of actual content for wire and electronic communications." Computer Crime and Intellectual Property Section, Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal

Investigation 71 (2001) available at http://www.cybercrime.gov/searchmanual.pdf.

A warrant is suggested, at a minimum, when an investigator wants to obtain access to opened voice mail, but the requirements of Title III apply if the investigator wants access to voice mail messages not yet retrieved by a subscriber or customer.

Nationwide Scope of Tools Used in Hacker Investigations

18 U.S.C. § 2703 (d) orders are nationwide in scope, as are subpoenas. Other tools used in hacker investigations contain express geographic limitations. Search warrants under Fed.R.Crim.P. 41(a), Title III orders permitting the interception of communications, and 18 U.S.C. § 3123 (a) orders authorizing the installation of pen registers and trap and trace devices all apply only within the jurisdiction of the court.

Search Warrants

Search warrants may be obtained to gain access to the premises where the hacker is believed to have evidence of the crime. Such evidence would include the computer used to commit the crime, as well as the software used to gain unauthorized access and other evidence of the crime. Suggested language for a search warrant for evidence of this type is available in the online manual prepared by CCIPS.

Analyzing Evidence from a Hacker's Computer

A seized computer may be examined by a forensic computer examiner to determine what evidence of the crime exists on the computer. The court order should specifically authorize this search. Many federal agencies have trained personnel on staff who are able to prepare a mirror image of everything in the memory of a seized computer – often including the memory of things the

computer owner thought had been erased. The computer examiner will prepare a detailed report regarding the information on the computer and should be able to testify as an expert at trial.

The Use of Traditional Investigative Techniques

Information obtained through the methods described above may reveal the subscriber or customer whose computer was used to conduct an intrusion. If it does, traditional investigative techniques may then be needed to determine who actually used the identified computer to commit the crime.

Due to the anonymity provided by the Internet, a suspected hacker may claim that someone else used his computer and assumed his identity at the time of the attack. It may be difficult to prove otherwise. For example, In a case charged in the District of Nebraska, the identity of the suspected hacker who defaced a newspapers webpage by adding a bogus story was obtained even though computer logs showing the IP address of the hacker came to a dead-end because the hacker has used an ISP that provided anonymous access to the internet. United States v. Lynch, 8:00CR344 (D. Neb. Indictment filed Dec. 14, 2000). The now-defunct www.worldspy.com, kept no records of its users. Similar services still exist, such as www.anonymizer.com.

In the Nebraska case, calls to people in the community with the same last name as the person who was the subject of the unflattering article led authorities to the subject of the article, and that person led the FBI to the suspected hacker. Using tools available to obtain evidence of cyber crimes, including traditional investigative techniques such as this, federal law enforcement officer will continue to track down hackers and bring them to justice.

ABOUT THE AUTHOR

Daniel A. Morris is an Assistant United States Attorney (AUSA) in the District of Nebraska and is the Computer and Telecommunications Coordinator (CTC).

Mr. Morris has been an AUSA since 1987. Before that he was a Senior Corporate Counsel for the Mutual of Omaha Companies.

Mr. Morris is the author of two books, the Nebraska Trial Handbook and Federal Tort Claims, both published by West Publishing Company. Has published articles in the Creighton Law Review and for several years, was a regular contributor to Case and Comment, a magazine for lawyers.

Mr. Morris thanks CCIPS attorney Richard Dowing for his comments and suggestions regarding this article and also thanks Patrick DeWall, a law clerk for the District of Nebraska for his assistance.

Updated page July 10, 2001
Usdoj-crm/mis/jam